编 者 的 话

本题解是根据N.贾柯勃逊著《抽象代数学》（卷1）基本概念所选的全部习题编写的，所用的符号、定理、公式都与该书一致。它是我们在教学过程中，为适应教学需要，更好地帮助同学较全面地理解全书服务的。

在编写出版过程中，得到系主任方德植教授及有关方面的热情支持和鼓励，特此致谢。本题解由几何代数教研室代数组杨锡安、佘明湍、杨照南、林大兴等同志编写。由于编者的水平有限，加上时间匆促，书中难免有不少缺点错误，恳请读者批评指正。

一九八〇年七月

目　　录

引论：从集合论来……，自然数系

习　题　1

1．求证：对于各个n都有$n^{+}\neq n$

〔证〕：令$N=\{n\mid n^{+}\neq n，n$是自然数$\}$

首先，$1\in N$，因为若$1\notin N$，即$1^{+}=1$，这就是说1的后继元素是1，也就是1是1的生成元素，这与Peano关于自然数公理iii)："自然数1无生成元"矛盾。所以N是含有1的自然数集合。

次设k是N中的任一元素，即$k^{+}\neq k$。若$k^{+}\notin N$，即有$(k^{+})^{+}=k^{+}$，由Peano公理iv)："若$a^{+}=b^{+}$，则$a=b$"得到$k^{+}=k$，这与假设k是N中之元矛盾，$\therefore k^{+}\in N$。再由Peano公理v)："自然数的每个集合，若它含有1，且含有这个集合每个元素的后继元素，则这集合含有一切自然数"知，N是自然数全体，即$n^{+}\neq n$对所有自然数成立。

习　题　2

1．设$a>b$，$c>d$，求证：$a+c>b+d$，$ac>bd$。

〔证〕：设P表示自然数集合，a，b，c，$d\in P$。

(1) $\because a>b$，$\therefore$方程$a=b+x$对于x有在P中的解，即$\exists m\in P$使得$a=b+m$。$\therefore a+c=(b+m)+c=(b+c)+m\cdots(*)$

同样，$\because c>d$，$\therefore\exists n\in P$，使得$c=d+n$。

$\therefore b+c=b+(d+n)=(b+d)+n\cdots\cdots(**)$

由（*）知$a+c>b+c$。

由（**）知$b+c>b+d$。

再由传递性即得$a+c>b+d$。

（2）$\because a=b+m$，$\therefore ac=(b+m)c=bc+mc\cdots(*)'$

$\because c=d+n$，$\therefore bc=b(d+n)=bd+bn\cdots(**)'$

$\because m, n, b, c\in P$，$\therefore mc, bn\in P$。

$\therefore$由（*）′知$ac>bc$。

由（**）′知$bc>bd$。

再由传递性即得$ac>bd$。

习　题　3

1．设$x>y$，求证$-x<-y$。

〔证〕：令$x=(\overline{a, b})$，$y=(\overline{c, d})$，$a, b, c, d\in P$。

$\because x>y$，即$(\overline{a, b})>(\overline{c, d})$，

$\therefore a+d>b+c$，由于在P中交换律成立

$\therefore d+a>c+b$。即$(\overline{d, c})>(\overline{b, a})$

$\because (\overline{d, c})=-(\overline{c, d})$，$(\overline{b, a})=-(\overline{a, b})$。

$\therefore -(\overline{c, d})>-(\overline{a, b})$，即$-y>-x$，亦即$-x<-y$。

习　题　4

1．整数的任一个非空集合S为下（上）有界的，其意义是说：对于S里的各个s，有一个整数b（B）存在，使$b\leqslant s$（$B\geqslant s$）．求证：这样的S含有一个最小（最大）元素。

〔证〕：先证任一非空的上有界的整数集S必含有最大元素．假定S_+表示S中全部正整数的集合。当$S_+\neq\varnothing$，考察集

合

$H=\{h \mid h \geqslant s_+$，$s_+$是$S_+$的任意元素$\}$

∵S上有界，所以S_+也上有界∴存在正整数h_1，对于S_+中的任意元素s_+，都有$h_1 \geqslant s_+$，∴$h_1 \in H$，故H是非空的自然数的集合，根据关于自然数的性质（O_4），H有最小的h_0存在，使得对任意的$h \in H$，都有$h \geqslant h$。此时，显然有$h_0 \in S_+$，因为若$h_0 \notin S^+$，则对所有的$s_+ \in S_+$，都有$s_+ < h_0$。

于是$s_+ \leqslant h_0+(-1)$。而$h_0+(-1)<h_0$。这与h_0最小的假定矛盾。

∵$S_+ \subseteq S$，∴$h_0 \in S$。h_0就是S的最大元素。

当$S_+=\varnothing$时，若$0 \in S$，显然0就是S的最大元素

若$0 \notin S$。考察集合

$S'=\{-s \mid s$为S的元素$\}$∵对于任意$s \in S$，都有$s<0$

∴$-s>0$。即S'是正整数（自然数）集合，由关于自然数的性质（O_4），S'有最小数$-s_0$，对于S'中任一元素$-s$，都有

$$-s \geqslant -s_0$$

∴$s_0 \geqslant s$，即s_0是S中的最大元素。

再证任一非空的下有界的整数集合S必含有最小元素。设s_1是S的一个下界，则对任意的$s \in S$都有$s_1 \leqslant s$，∴$-s_1 \geqslant -s$。∴$-s_1$是集合$S'=\{-s \mid s$是S的元素$\}$的上界，据前面所证，S'含有最大元素$-s_0$。即对S'中任一元素$-s$，都有$-s \leqslant -s_0$，∴$s \geqslant s_0$，即s_0是集合S的最小元素。

2．若$x \geqslant 0$，则命$|x|=x$，但若$x<0$，则命$|x|=-x$，求证

$$|xy|=|x|\,|y| \qquad |x+y| \leqslant |x|+|y|$$

〔证〕：先证第一式．1）若 x，y 有一为0，等式显然成立。因两边都是零。

2）若 x、y 异号，不妨设 $x>0$，$y<0$．则 $xy<0$ 于是 $|xy|=-(xy)$．而 $|x|=x$．$|y|=-y$．得 $|x||y|=x(-y)=-(xy)$．等式成立。

3）若 x、y 同号，则 $xy>0$．$|xy|=xy$．

分两种情形，都是正数时，$|x|=x$，$|y|=y$，得 $|x||y|=xy$。都是负数时，$|x|=-x$、$|y|=-y$．得 $|x||y|=(-x)(-y)=xy$．等式也成立。

再证第二式，1）若 x、y 异号，不妨设 $|x|\geqslant|y|$．则 $|x+y|\leqslant|x|$，于是 $|x+y|\leqslant|x|+|y|$．

2）若 x、y 同号，分两种情形，都是正数时，

$$|x+y|=x+y=|x|+|y|$$

都是负数时，$|x+y|=-(x+y)=(-x)+(-y)=|x|+|y|$．

习 题 5

1．求证：q 与 r 是唯一的

〔证〕：设 $a=bq_1+r_1$，$0\leqslant r_1<|b|$．

又 $a=bq_2+r_2$，$0\leqslant r_2<|b|$．

则 $bq_1+r_1=bq_2+r_2$．于是 $b(q_1-q_2)=r_2-r_1$，得 $|b(q_1-q_2)|=|r_2-r_1|$

若 $q_1-q_2\neq0$，则左边 $|b(q_1-q_2)|=|b||q_1-q_2|\geqslant|b|$ 而右边 $|r_2-r_1|<|b|$，此不可能。

故必 $q_1-q_2=0$．由 $b(q_1-q_2)=r_2-r_1$，得 $r_2-r_1=0$．即 $q_1=q_2$，$r_1=r_2$。

第一章　半群及群

习　题　6

1．在整数的集合里定义二元合成$f(x, y) = x + y^2$，求作所有导出的四元合成。

解：由$N(n) = \dfrac{(2n-2)!}{n!\,(n-1)!}$得$N(4) = 5$，记$(xy) = x + y^2$所导出的五种四元合成为

$((a_1a_2)a_3)a_4 = ((a_1 + a_2^2)a_3)a_4 = (a_1 + a_2^2 + a_3^2)a_4 = a_1 + a_2^2 + a_3^2 + a_4^2$;

$(a_1(a_2a_3))a_4 = (a_1(a_2 + a_3^2))a_4 = (a_1 + a_2 + a_3^2)a_4 = a_1 + a_2^2 + a_4^2 + 2a_2a_3^2 + a_3^4$;

$(a_1a_2)(a_3a_4) = (a_1 + a_2^2)(a_3 + a_4^2) = a_1 + a_2^2 + (a_3 + a_4^2)^2 = a_1 + a_2^2 + a_3^2 + 2a_3a_4^2 + a_4^4$

$a_1(a_2(a_3a_4)) = a_1(a_2(a_3 + a_4^2)) = a_1(a_2 + (a_3 + a_4^2)^2)$
$= a_1(a_2 + a_3^2 + 2a_3a_4^2 + a_4^4)$
$= a_1 + (a_2 + a_3^2 + 2a_3a_4^2 + a_4^4)^2 = a_1 + a_2^2 + 2a_2a_3^2 + 4a_2a_3a_4^2 + a_3^4 + 2a_2a_4^4 + 4a_3^3a_4^2 + 6a_3^2a_4^4 + 4a_3a_4^6 + a_4^8$

$a_1((a_2a_3)a_4) = a_1((a_2 + a_3^2)a_4) = a_1(a_2 + a_3^2 + a_4^2) = a_1 + (a_2 + a_3^2 + a_4^2)^2 = a_1 + a_2^2 + 2a_2a_3^2 + 2a_2a_4^2 + a_3^4 + 2a_3^2a_4^2 + a_4^4$.

2．对于一个给定的二元合成，我们可以用归纳法定义n个元素的简单积为a_1u或va_n，这里u为$a_2, \cdots, a_n$的简单积，v为a_1，…，a_{n-1}的简单积，证明：$\geqslant 2^r$个元素的任一个积

可看作r个元素（它们自身也是积）的简单积。

〔证〕：对r施行数学归纳法：

当$r=1$时，$\geqslant 2$个元素的任一个积，由给定的二元合成结果是一个元素，所以它可看为一个元素的简单积，命题成立。

设为$r=k$时，命题成立：即$\geqslant 2^k$个元素的任意一个积可看作k个元素的简单积，现证对$r=k+1$命题成立。
$\geqslant 2^{k+1}$个元素的任意一个积由合成最后结果总可表为$u\cdot v$。因为元素的个数$\geqslant 2^{k+1}$，所以u，v中至少有一个(不妨设u)所含元素的个数$\geqslant 2^k$，由归纳法假设，u可表示为k个元素的简单积，把v中所含元素全体看作一个简单积，所以$\geqslant 2^{k+1}$个元素的任意一个积可看作$k+1$个简单积，所以对于任意自然数r，命题成立。

习 题 7

1．命G为实数二维组（a，b）的全体，其中$a\neq 0$，如果G里的合成由公式

$$(a, b)(c, d)=(ac, bc+d)$$

来定义，验证：G是一个群。

〔证〕1)．设(a, b)，$(c, d)\in G$，$\because a\neq 0, c\neq 0$ $\therefore ac\neq 0$，且$bc+d$也是实数，$\therefore (a, b)(c, d)=(ac, bc+d)\in G$

2) $[(a,b)(c,d)](e,f)=(ac,bc+d)(e,f)$
$\quad=(ace,bce+de+f)$

$(a,b)[(c,d)(e,f)]=(a,b)(ce,de+f)$
$\quad=(ace,bce+de+f)$

$\therefore [(a,b)(c,d)](e,f)=(a,b)[(c,d)(e,f)]$.

3）(1,0)为G的恒等元，$\because (1,0)(a,b)$

$=(a,b)(1,0)=(a,b)$

4）$(a,b)^{-1}=(a^{-1},-ba^{-1})\in G$，$\because a\neq 0$，$\therefore a^{-1}$有意义。

$(a,b)(a^{-1},-ba^{-1})=(1,0)$，$(a^{-1},-ba^{-1})(a,b)$

$=(1,-b+b)=(1,0)$故G成群。

习 题 8

1．设半群的元素e适合$e^2=e$，这元素叫做同势元素（或幂等元素．）证明：群里的同势元素是$e=1$．

〔证〕：设e是群G的同势元素，则

$$e^2=e.$$

$\because e\in G$．$\therefore$存在$e^{-1}\in G$，把上式同右乘e^{-1}，则得

$$e^2e^{-1}=ee^{-1}=1，而e^2e^{-1}=e$$

$\therefore e=1$．

2．求证半群G如果具有下列性质，则成为群：

（i）G有一个右恒等元l_r，（ii）G的每个元a对于l_r有一个右逆元。

〔证〕：对任意的$a\in G$，由（ii），存在$b\in G$使得$ab=l_r$，现要证b对于l_r也是a的左逆元，即$ba=l_r$

$bab=b(ab)=bl_r=b$

$\because b\in G$，$\therefore$存在$c\in G$，使得$bc=l_r$，把上式两边同右乘c得

$babc=ba(bc)=bal_r=ba=bc=l_r$

即　$ba=l_r$………（＊）

再证右恒等元l_r也是左恒等元，即$l_ra=a$。

∵$l_r a = (ab)a = a(ba) = al_r = a$。

∴$l_r = 1$，由（*）知b是a的右逆元又是左逆元，∴b是a的逆元，∴G成群。

3．设G为半群，且对于元素a与b，方程$ax = b$及$ya = b$都可解，证明：G是一个群。

〔证〕：设$e \in G$是方程$ax = a$的解，即$ae = a$

对于G中的任意元b，方程$ya = b$在G中有解。

$yae = (ya)e = be$

$yae = y(ae) = ya = b$。∴$be = b$

即e是G的右恒等元。

又，方程$ax = e$在G中有解，∴群G中的任意元a关于右恒等元e都有右逆元，由第2题知G成群。

4．如果相消律在一个有限半群里成立，证明：这半群是一个群。

〔证〕：令$G = \{a_1, a_2, \cdots, a_n\}$（其中$a_i$各不相同）是一个有限半群，任取$a \in G$，作集合$G_1 = \{aa_1, aa_2, \cdots, aa_n\}$，显然$G_1$中的每个元素都是G中的元素，而且当$i \neq j$时，$aa_i \neq aa_j$。因如果$aa_i = aa_j$，由相消律成立即得$a_i = a_j$，这与假设矛盾。∴$G = G_1$

于是G中的任一元素都可表为$b = a_j$即方程$ax = b$在G中有解。同理可证$ya = b$在G中也可解。

由第3题知G成群。

习　题　9

1．验证：形状如（1，b）的二维组的子集合构成习题7的第1题里所述的群的一个子群。

〔证〕：令$H=\{(1,b)\mid b$是实数$\}$。

1）$(1,b)(1,c)=(1,b+c)\in H$。

2）$(1,0)\in H$，$(1,0)(1,b)=(1,b)(1,0)=(1,b)$。

3）$(1,b)^{-1}=(1,-b)\in H$。$(1,b)(1,-b)=(1,-b)(1,b)=(1,0)$，故H为G的子群。

2．求证：群G的一个子集合H成为一个子群的充要条件是a与b属于H时，$ab^{-1}\in H$。

〔证〕：必要性：设H是群G的子群，若$a,b\in H$，则$b^{-1}\in H$ $\therefore ab^{-1}\in H$。

充分性：i）若$b\in H$，则$1=bb^{-1}\in H$。ii）$1,b\in H$则$b^{-1}=1b^{-1}\in H$，iii）若$a,b\in H$，则$b^{-1}\in H$ $\therefore a(b^{-1})^{-1}=ab\in H$。故H为G的子群。

3．求证：群的任一个有限子半群必为一个子群（参看习题8第4题）

〔证〕：设H是群G的一个有限子半群，因相消律在G里成立，所以在H里也成立。由习题8第4题知H成群，即H是G的一个子群。

4．设以A表示G的各子群H的任一个集合，求证：交$\bigcap_A H$是一个子群。

〔证〕：设a、$b\in\bigcap_A H$则a、b属于各个H，$\because$各个H都是G的子群，$\therefore ab^{-1}\in$各个H $\therefore ab^{-1}\in\bigcap_A H$，故$\bigcap_A H$是G的一个子群。

5．设a是群G的任一个元素，求证：与a可交换的元素的集合G(a)是G的一个子群。

〔证〕：记$G(a)=\{b\mid a$为G中一固定元素，$b\in G$，$ab=ba\}$.则$1\in G(a)\because 1a=a1=a$。$\therefore G(a)$非空。

设b，$c\in G(a)$，则$ba=ab$。$ca=ac$。

$(bc)\cdot a=b(ca)=b(ac)=(ba)c=(ab)c=a(bc)$

$\therefore bc\in G(a)$

对于$b\in G(a)$。$\because ab=ba$，$\therefore b^{-1}abb^{-1}=b^{-1}bab^{-1}$

即得$b^{-1}a=ab^{-1}$。$\therefore b^{-1}\in G(a)$。

故G(a)是G的一个子群。

习　题　10

1．设$x\to x'$是一个同构，求证：1的象$1'$是第二个群的恒等元素，并且$(a^{-1})'=(a')^{-1}$。

〔证〕：设a是第一个群的任一个元素，它在同构映射下的象为a'。由同构关系有$(1\cdot a)'=1'a'$，而$(1\cdot a)'=a'$。

$\therefore 1'a'=a'$。

同理可证　$a'1'=a'$。$\therefore 1'$是第二个群的恒等元素。

$\because a'(a^{-1})'=(a\cdot a^{-1})'=1'$，$(a^{-1})'a'=(a^{-1}\cdot a)'=1'$

$\therefore (a^{-1})'=(a')^{-1}$。

2．映照$\theta\to e^{i\theta}$是否为R+到由绝对值为1的复数组成的乘法群上的一个同构呢？

〔证〕：这个映照不是同构映照。

$\because \theta\neq\theta+2k\pi, k=\pm1,\pm2,\cdots$，而$e^{i\theta}=e^{i(\theta+2k\pi)}$

即$\theta\to e^{i\theta}$不是1—1的。

习　题　11

1．设$\alpha=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$，$\beta=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$

计算$\alpha\beta$，$\beta\alpha$，及α^{-1}。

〔解〕$\alpha\beta=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$

$\beta\alpha=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}$

$\alpha^{-1}=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$

2．写出S_3的元素，并作出这个群的乘法表。

〔解〕：S_3的元素有3！＝6个：

$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，$\sigma_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$，$\sigma_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$，

$\sigma_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$，$\sigma_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$，$\sigma_6=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$。

它的乘法表如下：

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

3．验证下列变换成一个变换群：

$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$，$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$。

〔证〕：这三个变换就是上题中的σ_1，σ_4，σ_5，令$H=\{\sigma_1, \sigma_4, \sigma_5\}$由乘法表知$\sigma_1\sigma_1=\sigma_1\in H$，$\sigma_4\sigma_4=\sigma_5\in H$，$\sigma_5\sigma_5=\sigma_4\in H$。

$\sigma_1\sigma_4=\sigma_4\in H$，$\sigma_1\sigma_5=\sigma_5\in H$，$\sigma_4\sigma_5=\sigma_1\in H$。

∴H中任意二个元素的乘积仍为H的元素。

σ_1是H的恒等元素：$\sigma_1\sigma_4=\sigma_4\sigma_1=\sigma_4$，$\sigma_1\sigma_5=\sigma_5\sigma_1=\sigma_5$，$\sigma_1^{-1}=\sigma_1\in H$。$\sigma_4^{-1}=\sigma_5\in H$。$\sigma_5^{-1}=\sigma_4\in H$

∴H成变换群。

4．§6里那些个例子是变换群？

答：例8与例9中所述的群是变换群。

5．验证由法则$x\to ax+b$，$a\neq 0$给出直线的变换的集合成一个变换群。证明这个群与习题7第1题里给出的群是同构的。

〔证〕：记变换 $x\to ax+b$为$\sigma(a,b)$，令$T=\{\sigma(a,b)\mid x\sigma(a,b)=ax+b\}$

∵映照$x\to ax+b$显然是映上的且1－1的。

∴T是1－1变换的集合。又因

（i）任取$\sigma(a,b)$，$\sigma(c,d)\in T$。则

$x(\sigma(a,b)\sigma(c,d))=(ax+b)\sigma(c,d)=c(ax+b)+d=acx+bc+d=x\sigma(ac,bc+d)$

∴$\sigma(a,b)\sigma(c,d)=\sigma(ac,bc+d)\in T$。

（ii）$\sigma(1,0)$是T中的恒等元素：$\sigma(1,0)\sigma(a,b)=\sigma(a,b)\sigma(1,0)=\sigma(a,b)$

（iii）$\sigma(a^{-1},-a^{-1}b)\in T$是$\sigma(a,b)$的逆元素：

$\sigma(a^{-1},-a^{-1}b)\sigma(a,b)=\sigma(a,b)\sigma(a^{-1},-a^{-1}b)=\sigma(1,0)$故T为变换群。

记

令$\sigma(a,b)\to(a,b)=\sigma'(a,b)$

这个对应显然是1－1且映上的。

$\because \sigma(a,b)\sigma(c,d)=\sigma(ac,bc+d)$

$\therefore (\sigma(a,b)\sigma(c,d))'=\sigma'(ac,bc+d)=(ac,bc+d)$

而$\sigma'(a,b)\sigma(c,d)=(a,b)\cdot(c,d)=(ac,bc+d)$

$\therefore (\sigma(a,b)\sigma(c,d))'=\sigma'(a,b)\sigma'(c,d)$

∴这个对应是同构对应。

即变换群T与实数二维组（a,b），$a\neq 0$对于给定合成法所构成的群同构

6．验证由（x、y）→（x+a，0）所定义的平面上变换的全体关于积合成组成群。它是一个变换群吗？

〔证〕记变换（x，y）→（x+a，0）为σ_a，令$G=\{\sigma_a \mid a为实数\}$任取σ_a，$\sigma_b\in G$。

$(x,y)(\sigma_a\sigma_b)=(x+a,0)\sigma_b=(x+a+b,0)=(x,y)\sigma_{a+b}$

$\therefore \sigma_a\sigma_b=\sigma_{a+b}\in G$。

σ_0是G中的恒等元：$\sigma_0\sigma_a=\sigma_a\sigma_0=\sigma_a$

$\sigma_{-a}\in G$是σ_a的逆元：$\sigma_{-a}\sigma_a=\sigma_a\sigma_{-a}=\sigma_0$

又，变换的乘积当然满足结合律，故G成群。

但因(x,y)→(x+a,o)不是平面上映上的1－1的变换，故G不是一个变换群。

习　题　12

1．写出S_3的正则实现

〔解〕：依习题11第2题里的记号，并把σ_i简记为i，i=1，2，…6则S_3的(右)正则实现为：

$\sigma_1\to\sigma_{1r}=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$，$\sigma_2\to\sigma_{2r}=\begin{pmatrix}1&2&3&4&5&6\\2&1&5&6&3&4\end{pmatrix}$

$$\sigma_3 \to \sigma_{3r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}, \quad \sigma_4 \to \sigma_{4r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix}$$

$$\sigma_5 \to \sigma_{5r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}, \quad \sigma_6 \to \sigma_{6r} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

习 题 13

1．把12阶循环群的子群列成一表

〔解〕：设〔a〕是12阶循环群，$a^{12}=1$

则〔a〕的子群共有$d(12)=6$个，它们是：

〔a〕，〔a^2〕，〔a^3〕，〔a^4〕，〔a^6〕，〔a^{12}〕$=\{1\}$。

2．令$Z=$〔a〕是$r(<\infty)$阶循环群，求证：a^m的阶是$[m,r]/m=r/(m,r)$。

〔证〕：令$d=(m,\ \gamma)$表示m，r的最大公约数，于是有

$$m=dm_1,\quad \gamma=dr_1,\quad (m_1,\ \gamma_1)=1.$$

$\because (a^m)^{r/(m,r)}=(a^m)^{\frac{r}{d}}=(a^r)^{\frac{m}{d}}=(a^r)^{m_1}=1^{m_1}=1$

又假设s是使$(a^m)^s=1$的任意正整数，则

由$a^{ms}=1$有$\gamma \mid ms$。$\therefore d\gamma_1 \mid dm_1s$，$\gamma_1 \mid m_1 s$。

$\because (\gamma_1,\ m_1)=1$。$\therefore \gamma_1 \mid s$，即$\frac{\gamma}{d} \mid s$。

$\therefore \frac{\gamma}{d}$是使得$(a^m)^s=1$最小的正整数，$\therefore a^m$的阶为$\frac{\gamma}{d}=\frac{\gamma}{(m,\gamma)}$

又$\because [m,\gamma]$表示m与γ的最小公倍数，而$m\gamma=[m,\ \gamma]\cdot(m,\ \gamma)$，

$$\therefore \frac{[m,\ \gamma]}{m}=\frac{\gamma}{(m,\ \gamma)}\text{是}a^m\text{的阶}.$$

3．求证：γ阶循环群恰含有$\phi(\gamma)$个生成元素，这里$\phi(\gamma)$（欧拉(Euler)的ϕ函数）表示$<\gamma$而与γ互质（亦

即$(\gamma, h)=1$）的正整数h的个数。

〔证〕：设〔a〕是γ阶循环群，则a的阶数为γ，若a^m也是〔a〕的生成元，即$[a]=[a^m]$，必须且只须a^m的阶数也是γ。

由上题知，a^m的阶数为$\frac{\gamma}{(m,\gamma)}$，要使$\frac{\gamma}{(m,\gamma)}=\gamma$，必须且只须$(m,\gamma)=1$，即m与$\gamma$互质，因<$\gamma$而与$\gamma$互质的正整数个数为$\varphi(\gamma)$，故$\gamma$阶循环群恰有$\phi(\gamma)$个生成元素。

4。求证：下列两性质的每个都是γ阶循环群G的$t(\gamma=st)$阶子群H的特点：（1）H是G的元素的s幂的集合。

（2）H是能使$h^t=1$的元素h的集合。

〔证〕：设$G=[a]=\{1, a, a^2, \cdots a^{r-1}\}$是$\gamma$阶循环群，对$\gamma$的一个因子t，由§11定理4．G有唯一的t阶子群H，且 $H=[a^s]=\{1, a^s, (a^s)^2, \cdots (a^s)^{t-1}\}$

（1）现设H_1是G的元素的s幂集合：

$H_1=\{1, a^s, (a^2)^s, \cdots, (a^{r-1})^s\}=\{1, a^s, (a^s)^2, \cdots, (a^s)^{r-1}\}$

显然$H\subseteq H_1$，现要证$H_1\subseteq H$。

任取$(a^s)^m\in H_1$，令$m=pt+q$，$0\leqslant q<t$。

$(a^s)^m=(a^s)^{pt+q}=(a^{st})^p\cdot(a^s)^q=(a^r)^p\cdot(a^s)^q=(a^s)^q\in H$。

$\therefore H_1=H$

（2）设$H_2=\{h \mid h\in G, h^t=1\}$

任取$(a^s)^j\in H$则$((a^s)^j)^t=(a^{st})^j=(a^r)^j=1$。

$\therefore (a^s)^j\in H_2$。$\therefore H\subseteq H_2$。

任取$h=a^k\in H_2$。$0\leqslant k<\gamma$。则$(a^k)^t=a^{kt}=1$。

$\therefore \gamma \mid kt$。即$kt=l\gamma=lst$。

$\therefore k = ls$，即$h = a^k = a^{ls} = (a^s)^l \in H_1 = H$。

$\therefore H_2 \subseteq H$。故$H_2 = H$。

习 题 14

1．设将S_4的元素写成：（1）不相交循环的积。（2）对换的积。决定A_4的元素。

〔解〕

（1）

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1) \quad \alpha_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

$$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34) \quad \alpha_9 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$$

$$\alpha_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (234) \quad \alpha_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (123)$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (23) \quad \alpha_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1243)$$

$$\alpha_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (243) \quad \alpha_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (124)$$

$$\alpha_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24) \quad \alpha_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)$$

$$\alpha_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12) \quad \alpha_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1342)$$

$$\alpha_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13) \quad \alpha_{20} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (142)$$

$$\alpha_{16} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (134) \quad \alpha_{21} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (143)$$

$$\alpha_{17} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24) \quad \alpha_{22} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = (14)$$

$$\alpha_{18} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324) \quad \alpha_{23} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1423)$$

$$\alpha_{19} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432) \quad \alpha_{24} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

(2) $\alpha_1=(1)$, $\alpha_2=(34)$, $\alpha_3=(23)(24)$, $\alpha_4=(23)$

$\alpha_5=(24)(23)$ $\alpha_6=(24)$ $\alpha_7=(12)$, $\alpha_8=(12)(34)$

$\alpha_9=(12)(13)(14)$ $\alpha_{10}=(12)(13)$ $\alpha_{11}=(12)(14)$
(13). $\alpha_{12}=(12)(14)$, $\alpha_{13}=(13)(12)$ $\alpha_{14}=(13)(14)(12)$

$\alpha_{15}=(13)$, $\alpha_{16}=(13)(14)$, $\alpha_{17}=(13)(24)$

$\alpha_{18}=(13)(12)(14)$, $\alpha_{19}=(14)(13)(12)$, $\alpha_{20}=(14)$
(12). $\alpha_{21}=(14)(13)$, $\alpha_{22}=(14)$, $\alpha_{23}=(14)(12)(13)$

$\alpha_{24}=(14)(23)$.

A_4: $\{\alpha_1, \alpha_3, \alpha_5, \alpha_8, \alpha_{10}, \alpha_{12}, \alpha_{13}, \alpha_{16}, \alpha_{17}, \alpha_{20}$
$\alpha_{21}, \alpha_{24}\}$

2. 设$n\geqslant 3$,求证:A_n的任一个元素是三元循环(abc)的积

〔证〕:因A_n的任一元素都可表成偶数个对换的积,故只须证明任意两个对换的积可表成三元循环的积。

设(ab)、(cd)是任意二个对换。

(1)若(ab) = (cd),则(ab)(cd) = (ab)(ab) = 1.

∵$n\geqslant 3$,∴至少存在一个异于a、b的元c,使得

$$1=(abc)(abc)^{-1}=(abc)(acb)$$

(2)若a、b与c、d间有一个元素相同,不妨设a = c,则

$$(ab)(cd)=(ab)(ad)=(abd)$$

(3)若a、b与c、d都不相同,则

$$(ab)(cd)=(abd)(acd).$$

习　题　15

1. 在S_3里决定子群H = {1, (12)}的陪集分解

〔解〕:S_3 = {1, (12), (13), (23), (123), (132)}

$\because (13)H = \{(13), (132)\}$,

$(23)H = \{(23), (123)\}$.

$\therefore S_3$关于H的右陪集分解为

$$S_3 = H + (13)H + (23)H$$

又$\because H(13) = \{(13), (123)\}$

$H(23) = \{(23), (132)\}$,

$\therefore S_3$关于H的左陪集分解为

$$S_3 = H + H(13) + H(23)$$

2. 设V是平面上向量群，合成用向量加法，求证：由原点出发而终点在过O的一条定直线上组成一个子群，关于这个子群的陪集是什么？

〔证〕：设α为过原点的定直线l上的一个非零向量，由原点出发而终点在l上的向量全体记为H，则$H = \{k\alpha \mid k$是一切实数$\}$

显然，H是平面上向量群V的非空子集，又因为：

1）任取$k_1\alpha$，$k_2\alpha \in H$，则．$k_1\alpha + k_2\alpha = (k_1 + k_2)\alpha \in H$.　　（$\because k_1 + k_2$仍为实数）

2）$O = O \cdot \alpha \in H$是H的恒等元素：$k\alpha + O\alpha = k\alpha$.

3）对于$k\alpha \in H$，有逆元$-(k\alpha) = (-k)\alpha \in H$（$-k$是实数）

$$k\alpha + (-k)\alpha = O\alpha.$$

$\therefore$H关于向量加法构成V的子群。

V关于H的陪集$\beta + H$是始点在原点O终点在过向量β端点而平行于l的直线上的向量全体。

3. 设H_1与H_2是G的两个子群，求证：关于$H_1 \cap H_2$的任一个陪集是关于H_1的一个陪集与关于H_2的一个陪集的交.

利用这结果来证明庞加赖（Poincare′）定理：设H_1与H_2在G里有有限指数，则$H_1 \cap H_2$，也有有限指数。

〔证〕：只对右陪集情形证明，左陪集情形类同。

令$H = H_1 \cap H_2$，∵H_1，H_2是G的子群，∴H也是G的子群。

设$xH = \{xh \mid h \in H_1 \cap H_2, x \in G\}$。

现要证$xH = x(H_1 \cap H_2) = xH_1 \cap xH_2$

任取$xh \in xH$，∵$h \in H_1 \cap H_2$，∴$h \in H_1$且$h \in H_2$。

∴$xh \in xH_1$，$xh \in xH_2$，因而$xh \in xH_1 \cap xH_2$。

即。$xH \subseteq xH_1 \cap xH_2$。

反之，任取$a \in xH_1 \cap xH_2$，则$a \in xH_1$且$a \in xH_2$。

即a可表为$a = xh_1 = xh_2$，其中$h_1 \in H_1$，$h_2 \in H_2$

记

由相消律得$h_1 = h_2 = h$，∴$a = xh$。

∵$h \in H_1$且$h \in H_2$，∴$h \in H_1 \cap H_2$。

∴$a = xh \in x(H_1 \cap H_2) = xH$。

即$xH_1 \cap xH_2 \subseteq xH$。从而有$xH = xH_1 \cap xH_2$。

今利用这一结果证明庞加赖定理：

因为H_1与H_2在G里有有限指数，即H_1与H_2在G里不同陪集的个数是有限的，而$H_1 \cap H_2$在G里的每一个陪集都是关于H_1的一个陪集与关于H_2的一个陪集的交，所以$H_1 \cap H_2$在G里不同陪集的个数也是有限的。即。$H_1 \cap H_2$在G里的指数是有限的。

4. 法则$xH \to Hx$是否定义一个（单值）映照呢？

〔证〕：一般情况下，$xH \to Hx$不是一个（单值）映照。这是因为，如果$xH = yH$，即有$y^{-1}x \in H$。而要使$xH \to H$

x 能够定义一个映照，必须 $Hx = Hy$，也就是必须 $xy^{-1} \in H$ 但由于 y^{-1} 与 x 不一定能交换，所以 $y^{-1}x \in H$ 不能保证推出 $xy^{-1} \in H$，所以这个法则也就不一定能定义一个映照。

例如记 S_3 的子群 $S_2 = H = \{(1), (12)\}$. 由 $(23)H = (123)H = \{(23), (123)\}$ 而 $H(23) = \{(23), (132)\}$，$H(123) = \{(13), (123)\}$ 即 $H(23) \neq H(123)$ 故 $xH \to Hx$ 不是单值映照。

习 题 16

1．求证：任一个指数是 2 的子群是不变的。

〔证〕设H是群G的指数为 2 的子群，则G关于H的左右陪集分解为

$$G = H + Ha = H + aH. \quad (a \notin H)$$

因此，当 $a \notin H$ 时，有 $Ha = aH$。

当 $a \in H$ 时，$Ha = H$，$aH = H$，$\therefore Ha = aH$.

所以对G中的任意元 x，恒有

$$xH = Hx.$$

故H是G的不变子群。

2．求证：$H = \{1. (12)\}$ 在 S_3 里不是不变的.

〔证〕：取 $(2\ 3) \in S_3$，则.

$$(23)H = \{(23), (123)\}$$

而 $H(23) = \{(23), (132)\}$

$\therefore (23)H \neq H(23)$。

故H不是 S_3 里的不变子群。

3．求证：由 $x \to x + b$ 形的变换构成的子群在变换 $x \to ax + b\ (a \neq 0)$ 所成的群里是不变子群.

〔证〕：令$G=\{\alpha \mid x\alpha=ax+c,\ a\neq 0\}$，$H=\{\beta \mid x\beta=x+b\}$

∵H中的元是G中的元在 $a=1$ 的特殊情形，∴H是G的非空子集。又因为

1）任取$\beta,\gamma\in H$，由$x(\beta\gamma)=(x\beta)\gamma=(x+b)\gamma$
$$=x+b+c=x+(b+c)$$
推得$\beta\gamma\in H$。

2）恒等变换$1\in H$。（这时取$b=0$）

3）对于$\beta\in H$。有β^{-1}：$x\beta^{-1}=x+(-b)$，∴$\beta^{-1}\in H$。所以H是G的子群。

其次，对G中任意元α：$x\to ax+c$.（$a\neq 0$）及H中任意元β：$x\to x+b$，

$$\because x(\alpha^{-1}\beta\alpha)=(x\alpha^{-1})\beta\alpha=\left(\frac{1}{a}x-\frac{c}{a}\right)\beta\alpha$$
$$=\left[\frac{1}{a}(x+b)-\frac{c}{a}\right]\alpha=\left(\frac{x}{a}+\frac{b}{a}-\frac{c}{a}\right)\alpha$$
$$=\frac{1}{a}(ax+c)+\frac{b}{a}-\frac{c}{a}=x+\frac{b}{a}.$$

∴$\alpha^{-1}\beta\alpha\in H$，即$\alpha^{-1}H\alpha\subseteq H$。
故H是G的不变子群。

习　题　17

1．就前面各个例子决定同态核。

〔解〕（1）∵$\theta\to e^{i\theta}$是R_+到$U=\{e^{i\theta}\mid \theta$为实数$\}$上的一个同态。$e^{i2k\pi}=1$是U的恒等元，∴同态核为〔$2\pi$〕$=\{2k\pi \mid k$是整数$\}$。

（2）∵$(\alpha,\beta)\to\alpha$是V到R_+上的一个同态，而0是R_+

的恒等元，所以同态核为$\{(0,\beta)\mid\beta$为任意实数$\}$，即平面V上第二坐标轴上的全体向量所成的集合。

(3) $\because \tau \to x(\tau)=\begin{cases}1 & \text{当}\tau\text{是偶置换} \\ -1 & \text{当}\tau\text{是奇置换}\end{cases}$

是S_n到$\{1,-1\}$上的一个同构，而1是$\{1,-1\}$的恒等元，所以同态核为A_n（n次交代群）。

(4) 设a是群G的一个固定元素，$\because n \to a^n$是I_+到G内的一个同态，而1是G的恒等元素，所以同态核为

$$\begin{cases}0 & \text{当a是无限阶元} \\ [\gamma] & \text{当a是有限}\gamma\text{阶元}\end{cases}$$

2. 求证定理6的下面拓广：令G是一个群，而G′是定义有合成a′b′的任一个集合，假设η是G到G′内的任一个映照使，$(xy)\eta=(x\eta)(y\eta)$，则象Gη对于G′里所定义的合成来说成一个群。

〔证〕：1) 取$x\eta, y\eta\in G\eta$，$\because (x\eta)(y\eta)=(xy)\eta\in G\eta$。

$\therefore G\eta$关于G′里的合成是封闭的。

2) $\because$G是一个群，有$(xy)z=x(yz)$

$$\therefore [(x\eta)(y\eta)](z\eta)=[(xy)z]\eta=x(yz)\eta$$
$$=(x\eta)[(y\eta)(z\eta)]。$$

即Gη里的元关于G′的合成满足结合律。

3) $\because 1x=x1=x$，有$(1\eta)(x\eta)=(x\eta)(1\eta)=x\eta$ $\therefore 1\eta$是Gη里的恒等元素。

4) 对任意$x\eta\in G\eta$，则$(x\eta)^{-1}=x^{-1}\eta\in G\eta$。

而$(x\eta)(x^{-1}\eta)=(x^{-1}\eta)(x\eta)=(x^{-1}x)\eta=1\eta$。

所以Gη关于G′里所定义的合成来说构成群。

3. 求证：群R_+与例1的群U不同构。

〔证〕(反证)若$R_+\cong U$,记同构映射为φ,由同构性质知:
$\varphi(0)=1$,又$e^{i\pi}\neq 1$,设$\varphi(a)=e^{\pi i}$因φ是同构映射,
$\therefore a\neq 0$,但$\varphi(2a)=\varphi(a+a)=\varphi(a)\varphi(a)=e^{\pi i}\cdot e^{\pi i}=e^{2\pi i}$
$=1$,得$2a=0$与$a\neq 0$矛盾,故R_+与U不同构。

4. 令G是映照$x\to ax+b$所成的变换群,这里a与b是实数,而$a\neq 0$,求证:把上述的变换与实数a联结起来的对应是G到R^*上的一个同态。它的核是什么?

〔证〕:令$G=\{\alpha_{ab}\mid x\alpha_{ab}=ax+b, a,b$是实数,且$a\neq 0\}$.　　$R^*=\{a\mid a$是非零实数$\}$.

作映照η:$\alpha_{ab}\to a$,显然这是一个单值映照,而且对于R^*中任一元C,G中有α_{cb},使得$\alpha_{cb}\eta=c$. $\therefore\eta$是G到R^*上的单值映照。同时由于

$x(\alpha_{ab}\alpha_{cd})=(x\alpha_{ab})\alpha_{cd}=(ax+b)\alpha_{cd}=a(cx+d)+b=acx+ad+b$

$$\therefore(\alpha_{ab}\alpha_{cd})\eta=ac=(\alpha_{ab}\eta)\cdot(\alpha_{cd})\eta.$$

故η是G到R^*上的一个同态。

$\because R^*$的恒等元素是1,所以同态核为$G_1=\{\alpha_{1b}\mid x\alpha_{1b}=x+b$, b为任意实数$\}$.

5. 求证:如果k是一个非零整数,则映照$e^{i\theta}\to e^{ki\theta}$,是U到它自身上的一个同态,决定它的核。

〔证〕令映η:$e^{i\theta}\to e^{ki\theta}$是一个固定的非零整数,

$\because|e^{ki\theta}|=1$, $\therefore e^{ki\theta}\in U$, $\therefore\eta$是U到U内的单值映射,而对于U中的任一元$e^{i\theta}$,在U中有元$e^{i\frac{\theta}{k}}$,使$(e^{i\frac{\theta}{k}})\eta=e^{i\theta}$.

$\therefore\eta$是U到U上的单值映射。同时由于

$$(e^{i\theta_1}\cdot e^{i\theta_2})\eta=(e^{i(\theta_1+\theta_2)})\eta=e^{ki(\theta_1+\theta_2)}$$
$$=e^{ki\theta_1}\cdot e^{ki\theta_2}=(e^{i\theta_1}\eta)(e^{i\theta_2}\eta).$$

$\therefore \eta$ 是U到它自身上的一个同态。

$\because e^{kio}=e^{o}=1$ 是U的恒等元素.所以同态核 $\eta^{-1}(1)$ 是〔$e^{i\frac{2\pi}{k}}$〕，即由 $e^{i\frac{2\pi}{k}}$ 所生成的U里的循环群。

特殊情况：当 $k=0$ 时，则映照 η： $e^{ie}\to e^{kie}=e^{0}=1$ 是U到U内的一个同态，实际上是U到U的恒等元所成的子群 $\{1\}$ 上的一个同态，此时同态核即U本身。

习　题　18

1．求证：$R_+/〔2\pi〕\cong U$，这里 R_+ 及U的意义与§15的例1同．而〔2π〕是由 2π 生成的循环群。

〔证〕：由习题17第1题知，$\theta\to e^{i\theta}$ 是 R_+ 到U上的一个同态映照，且其同态核为〔2π〕，根据群的同态基本定理即得 $R_+/〔2\pi〕\cong U$。

2．令〔x〕是S阶循环群，〔y〕是t阶循环群，令 η 表〔x〕到〔y〕内的一个同态，使 $x\eta=y^k$．求证：这个映照存在，必须而且只须sk是t的倍数。设 $sk=mt$，求证：η 是一个同构必须而且只须 $(S, m)=1$。

〔证〕：(1)必要性：设 η 是〔x〕到〔y〕内的一个同态，满足 $x\eta=y^k$，则．

$$x^n\eta=\underbrace{x\eta\cdots x\eta}_{n\text{个}}=(y^k)^n=y^{nk}，（n为任意正整数）$$

且 $1_x\eta=1_y$．（1_x，1_y 分别为〔x〕，〔y〕的恒等元）

$\therefore 1_x\eta=x^s\eta=y^{sk}=1_y$．$\because$ y的阶数为t，故得 $t\mid Sk$。

充分性：设 $Sk=mt$．η： $x^n\to y^{nk}$ 显然是〔x〕到〔y〕内的一个对应，现假定 $x^i=x^j$，即 $x^{i-j}=1_x$，

$\because$ x的阶数为S，$\therefore S\mid i-j$．令 $i-j=sl$．则

$$ik-jk=(i-j)k=Sik=tml.$$

$$\therefore y^{ik-jk}=y^{tml}=(y^t)^{ml}=1_y。即 y^{ik}=y^{jk}.$$

故 η 是一个单值映照. 又因为

$$(x^i x^j)\eta=(x^{i+j})\eta=y^{(i+j)k}=y^{ik}\cdot y^{jk}=(x^i\eta)(x^j\eta).$$

所以 η 是〔x〕到〔y〕内的一个同态而且满足 $x\eta=y^k$.

（2）必要性：设 $sk=mt$. η 是〔x〕到〔y〕上的一个同态。满足 $x\eta=y^k$. 记 $(s,m)=d$，则

$$x^{\frac{s}{d}}\eta=\eta^{\frac{s}{d}k}=(y^t)^{\frac{m}{d}}=1_y$$

如果 η 是一个同构，必须 $x^{\frac{s}{d}}=1_x$，于是有 $s\mid\frac{s}{d}$，即 $d=(S\ m)=1$.

充分性：设有 $0\leqslant S_1<S$ 使 $x^{s_1}\eta=1_y$，即 $y^{s_1k}=1_y$，则 $t\mid s_1k \quad st\mid s_1ks, st\mid s_1mt$。$\therefore s\mid s_1m$，如果 $(s,m)=1$，则有 $s\mid s_1$。$\therefore s_1=0$，即 η 的同态核只含一个元 $x^0=1_x$。故 η 是一个同构。

习　题　19

1．求证：映照 $a\to a^{-1}$ 是一个自同构，必须而且只须G是交换群。

〔证〕：必要性：设映照 $a\to a^{-1}$ 是自同构，则

$$(ab)^{-1}=a^{-1}b^{-1}$$

而 $(ab)^{-1}=b^{-1}a^{-1}$，$\therefore a^{-1}b^{-1}=b^{-1}a^{-1}$

令 $a^{-1}=c$，$b^{-1}=d$，$\therefore cd=dc$，由于a、b是任意的，所以c、d也是任意的，即G是交换群。

充分性：若 $a^{-1}=b^{-1}$，则 $(a^{-1})^{-1}=(b^{-1})^{-1}$，即 $a=b$。又，对G中任意元C，在G中有元 C^{-1}，使 $C^{-1}\to(C^{-1})^{-1}=C$ 所以映照 $a\to a^{-1}$ 是G上的 1 － 1 映照。

$\because (ab)^{-1}=b^{-1}a^{-1}$,

而G是交换群,$b^{-1}a^{-1}=a^{-1}b^{-1}$,于是有$(ab)^{-1}=a^{-1}b^{-1}$

故映照$a\to a^{-1}$是G上的一个自同构。

2．求证：如果k是一个整数，而G是交换群，则$a\to a^k$是一个自向态。

〔证〕：$a\to a^k$显然是G到自身的一个单值映射。

因为G是交换群，所以$(ab)^k=a^kb^k$

故$a\to a^k$是G的一个自同态。

3．决定任一个循环群的自同构群。

〔证〕：设G＝〔a〕，φ_k是G上的一个自同构，满足

$\varphi_k(a)=a^k$.

对于任意的$a^i\in$〔a〕,$\varphi(a^i)=(\varphi(a))^i=(a^k)^i$

由此可见a^k也是生成元（即自同构映照把生成元变成生成元）

$\therefore$〔a〕＝〔a^k〕。

1）当〔a〕是无限阶时，则〔a〕的生成元只有a^{-1}及a自身，此时G的自同构映照只有$a\to a^{-1}$及$a\to a$，即G的自同构群$A=\{\varphi_1: a\to a;\ \varphi_{-1}: a\to a^{-1}\}$

2）当〔a〕是n阶有限群时，$\varphi_k(a)=a^k$，由习题13第3题知，a^k是〔a〕的生成元必须且只须$(k,n)=1$

此时G的自同构群$A=\{\varphi_k \mid \varphi_k(a)=a^k,(k,n)=1\}$

4．决定对称群S_3的自同构群。

解：先证群的自同构把群的n阶元变为n阶元：

设φ是群G的自同构，a是G的n阶元，要证$\varphi(a)=b$也是G的n阶元。设b的阶为m。

$\because \varphi(1)=\varphi(a^n)=(\varphi(a))^n=b^n=1$，$\therefore m\mid n$

又$\because \varphi(a^m)=(\varphi(a))^m=b^m=1$.

因此，$m=n$。即b的阶数与a的阶数相同。

在对称群S_3中，(12)，(13)，(23)是它的二阶元；S_3的自同构只能把这三个二阶元变到这三个元，所以S_3的自同构最多只能有$3!=6$个。

因为S_n（$n>2$）的心是恒等元素，S_3的心只能是(1)由§17定理9知，S_3的内自同构群$I\cong S_3/(1)$，即S_3有6个互不相同的内自同构，故S_3的自同构群恰好由它的六个内自同构组成，因S_3没有外自同构。

5．由自同构群及右乘变换群生成的变换群H，叫做群G的全形群。求证：

（1）H包含所有左乘变换

（2）H的任一个元素必能而且只能有一个方法写做一个自同构α与一个右乘变换a_r的积αa_r。

（3）如果G是有限群，则H的阶是G的阶与A（G的自同构群）的阶的积。

〔证〕：（1）设a_l是由任意的$a\in G$所决定的左乘变换，对任意$x\in G$，

$$x a_l = a x = (a x a^{-1})a = (x c_{a^{-1}})a_r = x(c_{a^{-1}}a_r)$$

（这里，$c_{a^{-1}}$是由a^{-1}所决定的内自同构，a_r是由a决定的右乘变换）

$$\therefore a_l = c_{a^{-1}}a_r \in H.$$

即G的任意左乘变换都含于G的全形群中。

（2）先证任一个右乘变换a_r与一个自同构α的积可表为一个自同构β与一个右乘变换b_r的积，即$a_r\alpha=\beta b_r$。事实上，

$$x(a_r\alpha) = (x a_r)\alpha = (x a)\alpha = (x\alpha)(a\alpha) = x(\alpha(a\alpha))$$

$\therefore a_r\alpha=\alpha\ (a\alpha)$，只要取$\beta=\alpha$，$b_r=a\alpha$

即有$a_r\alpha=\beta b_r$.

因为H中的任一个元素是有限个元素的乘积，其中一部分是自同构，一部分是右乘变换，由于上面所证，可实行调换，使得前面的元素都是自同构，后面的元素都是右乘变换。因为有限个自同构的乘积仍是自同构，有限个右乘变换的乘积仍是右乘变换，所以H的任一元素可表为一个自同构与一个右乘变换的乘积。

现证表法的唯一性。

设$h\in H$，若$h=\alpha a_r=\beta b_r$，则对任意$x\in G$，有

$$x(\alpha a_r)=(\beta b_r)，即(x\alpha)a=(x\beta)b$$

特别取$x=1\in G$，$\because 1\alpha=1$，$1\beta=1$，代入上式即得

$$a=b \qquad \therefore a_r=b_r$$

又，把等式$(x\alpha)a=(x\beta)a$的两边同右乘以a^{-1}，则得

$$x\alpha=x\beta，即\alpha=\beta.$$

因此唯一性得证。

（3）因为G是有限群，所以G的自同构群A也是有限群由（2），H可表为$H=\{\alpha a_r \mid \alpha\in A，a_r为G的右乘变换\}$，H的阶由不同的元$\alpha a_r$的个数决定，因为$\alpha$与$\beta$，a与b两组中只要有一组不相同，则$\alpha a_r$与$\beta b_r$就不相同，所以不同的元$\alpha a_r$的个数等于$\alpha$所有可能的取值与$a_r$所有可能取值的乘积，即H的阶等于A的阶数与G的阶数的乘积。

习 题 20

1．求证：如果G是一个有限置换群，则由G决定的任一个传递集合里的元素个数是群的阶数的一个因子。

（提示：如果i是集合S＝｛1，2，…，n｝里任一个数目，则G里使i不变的变换α的集合是一个子群H。证明：含有i的传递集合里的元素可与H的左陪集成1—1对应，然后证明，传递集合里元素的个数是H在G里的指数）

〔证〕：设G是S＝｛1，2，…，n｝上的有限置换群，考虑集合

$$H=\{\alpha \mid \alpha\in G,\ i\alpha=i,\ i\in S\}$$

任取α，$\beta\in H$，则$i\alpha=i$，$i\beta=i$，

∵β是S上的1—1变换，∴$i\beta^{-1}=i$，于是

$i(\alpha\beta^{-1})=(i\alpha)\beta^{-1}=i\beta^{-1}=i$，∴$\alpha\beta^{-1}\in H$，因此H构成G的子群。

设x是含有i的传递集合里任一元素，即$x\equiv i\,(\mathrm{mod}G)$则存在$\alpha\in G$，使得$x=i\alpha$。

因H中任意元都使i保持不动，∴$x=i\alpha=iH\alpha$。

令$x\to H\alpha$，则这个映照是1—1的，且是映上的。事实上，设$y=i\beta=iH\beta$，∵$\alpha\beta\in G$，∴若$x=y$，显然有$\alpha=\beta$，即$H\alpha=H\beta$。

反之，若$H\alpha=H\beta$，则$\beta\alpha^{-1}\in H$。

由$y=i\beta$，有$y\alpha^{-1}=i\beta\alpha^{-1}=i(\beta\alpha^{-1})=i$

$$\therefore y=i\alpha=x。$$

而且，对任意一个$\gamma\in G$（即任意一个$H\gamma$），都有一个$i\gamma=z$与之对应，z属于含有i的传递集。

于是$x\to H\alpha$是含有i的传递集里的元素到H的左陪集的集合上的一个1—1对应。而G中H的不同左陪集的个数等于H在G中的指数，当G是有限群时，H在G中的指数是G的阶的一个因子，因此含有i的传递集的元素个数是群的阶数

的一个因子。

2．求证：在一个有限群G的任一个共轭类里，元数的个数是G的阶数的一个因子。

〔证〕：设G是有限群，a是G的任一元素，考虑集合

$$H_a=\{x \mid xa=ax,\ a\in G\}$$

任取x，y∈H_a，则xa=ax，ya=ay，而且

$y^{-1}yay^{-1}=y^{-1}ayy^{-1}$，即$ay^{-1}=y^{-1}a$，即$y^{-1}\in H_a$。

$a(xy^{-1})=(ax)y^{-1}=(xa)y^{-1}=x(ay^{-1})$
$=(xy^{-1})a$。

$\therefore xy^{-1}\in H_a$，因此H是G的子群。

设x是含有a的共轭类里的任一元素，则存在b∈G，使得

$$x=b^{-1}ab$$

令$x=b^{-1}ab\to Hb$，则这个映照是1—1的，且是映上的，事实上，设$y=c^{-1}ac\to Hc$，若x=y，即$b^{-1}ab=c^{-1}ac$则$c(b^{-1}ab)b^{-1}=c(c^{-1}ac)b^{-1}$，$(cb^{-1})a=(cb^{-1})$
$\therefore cb^{-1}\in H$。

$\therefore Hcb^{-1}=H$，即$HC=Hb$。

反之，若HC=Hb，则$cb^{-1}\in H$，即$a(cb^{-1})=(cb^{-1})a$。

$\therefore c^{-1}(acb^{-1})b=c^{-1}(cb^{-1}a)b \quad c^{-1}ac=b^{-1}ab$。

即x=y。

而且对任意的d∈G（即任意的Hd），总有$d^{-1}ad=z$与之对应，z属于含有a的共轭类。

于是$b^{-1}ab\to Hb$是含有a的共轭类到H的左陪集上的一个1—1对应，而G中H的不同左陪集的个数等于H在G中的指数，当G是有限群时，H在G中的指数是G的阶的一个因

因子，因此含有a的共轭类的元数个数是群G的阶数的一个因子。

3．求证：阶数是素数幂的群的心所含元素多于1个。

〔3〕：设群G的阶数为p^n，这里p是素数，n是正整数。把群按共轭进行分类。因为群的心的每个元素都是一个共轭类，所以如果G的心含有p_0个元，则G就有p_0个只含一个元素的共轭类。设其他的共轭类为G_i，（i＝1，2，…，γ，由第2题知，每个G_i的元素都是p^n的因子，设G_i的元数为p^{m_i}，$0<m_i\leqslant n$（i＝1，…，γ）于是得到关系式：

$$p^n = p_0 + p^{m_1} + \cdots + p^{m_r}$$ 即

$$p_0 = p^n - (p^{m_1} + \cdots + p^{m_r}) = p[p^{n-1} - (p^{m_1-1} + \cdots + p^{m_r-1})]$$

如果p_0＝1；则有$p[p^{n-1} - (p^{m_1-1} + \cdots + p^{m_r-1})] = 1$.

而因得出$p \mid 1$，因p是素数，这是不可能的。因此必须$p_0>1$，即群的心所含元素多于1个。

第二章　环.整区及域

习　题　21

1．令A是$(-\infty, \infty)$上所有实值函数的集合，求证：A对于通常加法是一个群，而对于$f\cdot g(x) = f(g(x))$是一个半群。A关于这两个合成是否成一个环呢？

〔证〕记$A = \{f(x) \mid x \in (-\infty, \infty), f(x) \in R\}$，任取f，g，h∈A.

（1）A对于通常加法：$(f+g)(x) = f(x) + g(x)$成群。这是因为

（i）$(f+g)(x)=f(x)+g(x)$仍是$(-\infty, \infty)$上的实值函数，即$f+g\in A$。

（ii）$[(f+g)+h](x)=(f+g)(x)+h(x)=f(x)+g(x)+h(x)$

$[f+(g+h)](x)=f(x)+(g+h)(x)=f(x)+g(x)+h(x)$

$\therefore (f+g)+h=f+(g+h)$

（iii）$0(x)\equiv 0$是A中关于加法的恒等元：

$(f+0)(x)=(0+f)(x)=f(x)$

（iv）对于$f\in A$，A中有f关于加法的逆元$-f$，使得

$[f+(-f)](x)=[(-f)+f](x)\equiv 0$。

（2）A对于乘法：$f\cdot g(x)=f(g(x))$ 成半群，这是因为

（i）$f(g(x))$是f，g的复合函数，它仍是$(-\infty, \infty)$上实值函数，即$f\cdot g\in A$。

（ii）$[f\cdot(g\cdot h)](x)=f[(g\cdot h)(x)]=f\{g[h(x)]\}$

$[(f\cdot g)\cdot h](x)=(f\cdot g)[h(x)]=f\{g[h(x)]\}$

$\therefore f\cdot(g\cdot h)=(f\cdot g)\cdot h$。

（3）A关于上述两个合成法不构成环。这是因为A虽然对加法成群，对乘法：$f\cdot g(x)=f(g(x))$成半群，但它不满足加法对乘法的分配律：

$f\cdot(g+h)(x)=f[(g+h)(x)]=f[g(x)+h(x)]$

而$(fg+fh)(x)=fg(x)+fh(x)=f[g(x)]+f[h(x)]$。

$\because$一般情况下，$f[g(x)+h(x)]\neq f[g(x)]+f[h(x)]$。

$\therefore f(g+h)\neq fg+fh$

2．求证：如果在三个元素0，1，2的集合里定义加

法及乘法如下表

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

则它成一个环。

〔证〕（1）由（+）表及（×）表可看出，这二种合成法其实是普通的加法及乘法，只是合成结果用关于模3的同余来表示，所以关于运算的结合律以及加法对乘法的分配律都成立。

（2）由（+）表可见，0，1，2三个元关于加法合成结果仍是0，1，2三个元，所以{0，1，2}关于加法封闭；由表的对称性可知，任二个元的合成是可交换的；0为恒等元素；0，1，2关于加法的逆元分别为0，2，1。因此{0，1，2}关于加法成群。

（3）由（×）表可见，0，1，2三个元素关于乘法合成结果仍是0，1，2三个元素，所以{0，1，2}关于乘法封闭。因此{0，1，2}关于乘法成半群。

由（1），（2），（3）即知{0，1，2}关于"+""×"成环。

习 题 22

1．求证：$a(b-c)=ab-ac$。

〔证〕：$a(b-c)=a(b+(-c))=ab+a(-c)$

$$=ab+(-ac)=ab-ac.$$

2．求证：对于任一个整数n，$n(ab)=(na)b=a(nb)$。

〔证〕：当$n=0$时，$0(ab)=0$，$(0a)b=0b=0$，

$a(ob)=ao=o$，　$\therefore o(ab)=(oa)b=a(ob)$。

当n为正整数时，

$$n(ab)=\underbrace{ab+ab+\cdots+ab}_{n个}$$

$$(na)b=(\underbrace{a+a+\cdots+a}_{n个})b=\underbrace{ab+ab+\cdots+ab}_{n个}$$

$$a(nb)=a(\underbrace{b+b+\cdots+b}_{n个})=\underbrace{ab+ab+\cdots+ab}_{n个}$$

$\therefore n(ab)=(na)b=a(nb)$

当n为负整数时，令$n=-n'$，n'为正整数。

$$n(ab)=-n'(ab)=-(\underbrace{ab+ab+\cdots+ab}_{n'个})$$

$$(na)b=(-n'a)b=-(\underbrace{a+a+\cdots+a}_{n'个})b=-(\underbrace{ab+\cdots+ab}_{n'个})$$

$$a(nb)=a(-n'b)=a[-(\underbrace{b+b+\cdots+b}_{n'个})]=-[a(\underbrace{b+\cdots+b}_{n'个})]$$

$$=-(\underbrace{ab+ab+\cdots+ab}_{n'个})\therefore n(ab)=(na)b=a(nb)$$

$\therefore$对任意整数n，均有$n(ab)=(na)b=a(nb)$。

3．令A是一个代数系，适合环的所有条件，只把加法的交换性除外，如果A含有一个元素c，它可以左相消，亦即如果$ca=cb$，则$a=b$，求证：A是一个环。

〔证〕：只要证对于任意a，b∈A，有a+b=b+a就可以了。

$$\because ca+cb-cb-ca=0$$

$$\therefore c(a+b)+(-c)(b+a)=0$$

即 $c(a+b)+[-c(b+a)]=0$

$$\therefore c(a+b)=c(b+a)$$

由已知，对c可实行左相消，即得a+b=b+a

习　题　23

1．求证：如果a是带恒等元素环的一个单位元素，则－a也是单位元素，证明：$(-a)^{-1}=-a^{-1}$

〔证〕：设环A有恒等元素1．因a是A的单位元素，则必有$a^{-1}\in A$使得

$$aa^{-1}=a^{-1}a=1.$$

因A是环∴ $-a\in A$，$-a^{-1}\in A$

且$(-a)(-a^{-1})=-[a(-a^{-1})]=aa^{-1}=1$

$$(-a^{-1})(-a)=-[a^{-1}(-a)]=a^{-1}a=1$$

所以－a也是单位元，而且

$$(-a)^{-1}=-a^{-1}.$$

2．求证：习题21的第2题里所给的代数系是一个域

〔证〕：在习题21的第2题中，我们已证所给的代数系是环，而且由（×）表看出0·1=1·0=0，0·2=2·0=0，1·2=2·1=2所以它是可换环

又因为｛0，1，2｝非零元素集合｛1，2｝关于乘法“×”封闭，1是它的恒等元，1，2的逆元分别是它们自己，所以它构成｛0，1，2｝乘法半群的子群。因此这个代

数系是可换除环，即它是一个域。

3．求证：任一个有限整区是一个除环。

〔证〕：设A是任一有限整区，考虑A中非零元的集合A^*，因为对于$a,b\in A^*$，a，b不是零因子，$\therefore ab\neq 0$，即$ab\in A^*$因此A^*是A的乘法半群的子半群。现只要证A^*成群即可。因A有限，所以A^*也有限，又A是整区，所以狭义相消律在A中成立，因A^*中都是非零元，所以在A^*中相消律成立。由第一章习题8第4题“如果相消律在有限半群里成立，则这个半群是一个群”可知，A^*是A的乘法半群的子群，因此A是一个除环。

4．求证：如果整区A有一个同势元素$e\neq 0$ $(e^2=e)$，则e是A的恒等元素。

〔证〕：设a是整区A中任一元，由于e是A的同势元素，所以有

$$ae=ae^2=(ae)e.$$

因为A是整区，狭义右相消律成立，此时$e\neq 0$，

$$\therefore a=ae.$$

同样，因为狭义左相消律成立，所以由$ea=e(ea)$得

$$a=ea.$$

即证得e是A的恒等元素。

5．如果环里一个元素适合$z^n=0$，这元素叫做无势元素（或叫幂零元素）．求证：整区的唯一无势元素是$z=0$．

〔证〕：设z是整区A的任一元，若$z=0$，显然有

$$z^n=0$$

所以0是A的无势元素．

若$z\neq 0$，用数学归纳法证明$z^n\neq 0$，

当$n=2$时，因A是整区，它不含有非零的零因子。

$\therefore z^2=z\cdot z\neq 0$。

设当$n=k$时，$z^k\neq 0$，则$z^{k+1}=z^k\cdot z\neq 0$。

$\therefore$当$z\neq 0$时，对任意自然数n，恒有$z^n\neq 0$。

这就是说，A中任意非零元都不是无势元素，所以整区A的无势元素只能是$z=0$。

6．如果一个环只有左恒等元1_l，求证1_l是（双侧）恒等元素。

〔证〕：若环A只含一个元素0时，则0既是左恒等元又是右恒等元，若A不只含一个元素时，显然它的左恒等元不是0元。对任意的$b\in A$，由于

$$(a1_l-a+1_l)b=a1_lb-ab+1_lb=ab-ab+b=b$$

（a为A中任一元）。

$\therefore a1_l-a+1_l$是一个左恒等式，由于A只有一个左恒等元1_l，

$\therefore a1_l-a+1_l=1_l$。

$a1_l-a=0$

即$a1_l=a$。

因此1_l也是A的右恒等元，即1_l是A的恒等元

7．令u是带恒等元素环的一个元素，它有一个右逆元素，

求证：下面关于u的各个条件都是等价的。

（1）u拥有不只一个的右逆元素

（2）u不是一个单位元素．

（3）u是一个左零因子。

〔证法一〕：（1）⇨（2）用反证：若u是一个单位元素，

则存在一个元素v，使得$uv=vu=1$，此时v就是u唯一的右逆元，因为若u还有一个右逆元v'，则$v'=(vu)v'=v(uv')=v\cdot 1=v$所以如果u不只有一个右逆元，则它一定不是单位元。

（2）⇨（3）由已知，u有一个右逆元v：$uv=1$.

因为u不是单位元，$\therefore vu\neq 1$. 即$vu-1\neq 0$.

又$\because u(vu-1)=uvu-u=u-u=0$.

$\therefore$ u是一个左零因子.

（3）⇨（1）若u是一个左零因子，则必存在$v\neq 0$，使

$$uv=0.$$

设v'是u的一个右逆元：$uv'=1$. 则由于

$$u(v+v')=uv+uv'=0+1=1.$$

$\therefore v+v'$也是u的右逆元，而且$\because v\neq 0$，$\therefore v+v'\neq v'$

即证得u拥有不只一个右逆元。

〔证法二〕：（1）⇨（3）．$\because$ u拥有不只一个右逆元，设a，b是它的两个不相同的右逆元，

即 $ua=1$，$ub=1$，

于是$ua=ub$，$u(a-b)=0$，$a-b\neq 0$.

$\therefore$ u是一个左零因子。

（3）⇨（2）$\because$ u是个左零因子，$\therefore$存在$b\neq 0$，使

$ub=0$.

若u是个单位元，即存在u'，使$uu'=u'u=1$.

于是$b=1\cdot b=(u'u)b=u'(ub)=u'\cdot 0=0$.

与$b\neq 0$矛盾.

$\therefore$ u不是一个单位元。

（2）⇨（1）$\because$ u不是单位元，已知a是u的一个右逆

元，

$\therefore ua=1$。但$au\neq 1$。

则　　$a+1-au\neq a$.

又$u(a+1-au)=ua+u-uau=ua+u-1\cdot u=ua=1$

即$a+1-au\neq a$又是u的一个右逆元.

8．卡浦兰斯基（Kaplansky）定理：如果带恒等元素环的一个元素拥有不只一个右逆元素：则它有无数个右逆元素。

〔证法一〕：设u是带恒等元素环A的一个元，如果它只有有限个右逆元，可假定它全部互异的右逆元有n个：$v_1,\cdots,v_n$,则有$uv_i=1$，（$i=1,2,\cdots,n$。）令$a_i=v_1+v_iu-1$

因$ua_i=u(v_1+v_iu-1)=uv_1+uv_iu-u=1+u-u=1$。

$\therefore a_i$（$i=1,2,\cdots,n$）也是u的右逆元，这n个右逆元也互不相同，即当$i\neq j$时，$a_i\neq a_j$，因为若$a_i=a_j$，则有.

$v_1+v_iu-1=v_1+v_ju-1$

即　　$v_iu=v_ju$.

两边同右乘以v_1得$v_i=v_j$，这与$v_i.v_j$互异的假设矛盾.其次a_i也与v_1不相同。若不然，由

$v_1=v_1+v_iu-1$

得$v_iu=1$。这说明v_i是u的右逆元又是左逆元，所以u是单位元，但由已知u拥有不只一个右逆元，据第7题，u不可能是单位元，从而得出矛盾。

于是得到v_1，a_1，…，a_n这$n+1$个互异u的右逆元，这与假设u只有n个右逆元矛盾．所以u如果有不止一个右逆元，则必有无数个右逆元。

〔证法二〕：设u拥有不只一个右逆元。

记$X=\{x \mid ux=1\}$是u的右逆元的集合，即X至少含有两个元素。由上题知，u不是单位元，∴u没有左逆元。

取$x_0 \in X$是某个固定元，记$Y=\{xu-1+x_0 \mid x \in X\}$。

∵$u(xu-1+x_0)=(ux)u-u+ux_0=1\cdot u-u+1=1$。

∴$xu-1+x_0 \in X$。即$Y \subseteq X$。
又$x_0 \in X$。今证$x_0 \bar{\in} Y$。

否则X中有元x，使$x_0=xu-1+x_0$，得$xu-1=0$，$xu=1$。与u没有左逆元矛盾。∴$Y \subset X$

今在X与Y间建立对应η：$x \in X$　　$x\eta=xu-1+x_0 \in Y$。显然η是单值的。

若$x\eta=y\eta$，即$xu-1+x_0=yu-1+x_0$，得$xu=yu$　　$x(ux_0)=y(ux_0)$，∴$x=y$，故η是一对一的。而X与它的真子集Y间存在一个一对一对应关系，只能当X是无穷集时才有可能。故X是无穷集。

习　题　24

1．如果e是同势元素，求证：$e\circ e=e$。于是，求证：如果e是右拟正则元素，则$e=0$。

〔证〕：设e是同势元素，则有$e^2=ee=e$。

∴$e\circ e=e+e-ee=e+e-e=e$。

如果e又是右拟正则元素，则存在e'，使得，

$e\circ e'=0$

两边与e作园合成得

$e\circ(e\circ e')=e\circ 0=e$。

而 $e\circ(e\circ e')=(e\circ e)\circ e'=e\circ e'=0$.

$\therefore e=o$.

2. 求证：任一个无势元素属于Q.

〔证〕：设a是环A的无势元素，则 $a^n=o$.

若 $n=1$，则 $a=o$，$\because O\circ O=O$ $\therefore O$是拟正则元. 即 $a=o\in Q$.

若 $n>1$. 取 $b=-(a+a^2+\cdots+a^{n-1})$，因为

$$a\circ b=a\circ[-(a+a^2+\cdots+a^{n-1})]$$

$$=a+[-(a+a^2+\cdots+a^{n-1})]+a(a+a^2+\cdots+a^{n-1})=a^n=0.$$

同样 $b\circ a=-(a+a^2+\cdots+a^{n-1})\circ a=a^n=0$.

$\therefore b$是a的拟逆元，即a是拟正则元，$\therefore a\in Q$.

3. 求证：卡浦兰斯基关于一个除环的特性的定理：一个环的元素，除一个元素是例外，其余都有一个右拟逆元素。

〔证法一〕：必要性：设A是除环，则A含有恒等元素1，因为对任意 $b\in A$

$$1\circ b=1+b-1\cdot b=1\neq 0$$

$\therefore 1$没有右拟逆元。而对任意 $a(\neq 1)\in A$.

$1-a(\neq o)\in A$，$\because A$是除环，$\therefore (1-a)$有逆元记为 $1-a'$ 即

$$1=(1-a)(1-a')=1-a-a'+aa'.$$

$\therefore a+a'-aa'=0$. 即 $a\circ a'=0$.

a'是a的右拟逆元。因此，除环A除了恒等元外，其余的元都有一个右拟逆元。

为证充分性，先证下列

引理 若a的右拟逆元是b，而b本身也有右拟逆元c，则c=a。事实上，由

$$a\circ b=a+b-ab=0 \cdots\cdots\cdots\cdots ①$$

$$b\circ c=b+c-bc=0 \cdots\cdots\cdots\cdots ②$$

可得 $a-ab=c-bc \cdots\cdots\cdots\cdots ③$

把①右乘以c，②左乘以a得

$$ac+bc-abc=o\cdot c=0 \cdots\cdots\cdots\cdots ①'$$

$$ab+ac-abc=a\cdot o=0 \cdots\cdots\cdots\cdots ②'$$

由①'，②'可得ab=bc。把此式代入③即证得

$$a=c。$$

现证充分性：

（1）设e是A中唯一没有右拟元的元，显然 $e\neq 0$，先证e是A的左恒等元，若不然，必存在 $x\in A$，使得 $ex\neq x$，于是有

$$e+ex-x\neq e。$$

由假设，$e+ex-x$ 有右拟逆元，记为y，则。

$$O=(e+ex-x)\circ y=e+ex-x+y-(e+ex-x)\cdot y$$

$$=e+ex-x+y-ey-exy+xy$$

$$=e+(y-x+xy)-e(y-x+xy)$$

$$=e\circ(y-x+xy)$$

即 $e\circ(y-x+xy)=0$。这与e没有右拟逆元矛盾。所以e是A的左恒等元，从而有 $e^2=ee=e$。

再证e是A的右恒等元。若不然，必存在 $x\in A$，使得 $xe\neq x$，于是有 $e+x-xe\neq e$

由假设 $e+x-xe$ 有右拟逆元，记为y，我们断言 $y\neq e$。因为如果 $y=e$。则

$$0=(e+x-xe)\circ e=e+x-xe+e$$
$$-(e+x-xe)\cdot e=e+x-xe+e-e^2-xe+xe^2$$
$$=e+x-xe+e-e-xe+xe=e+x-xe.$$
把$e+x-xe=0$两边右乘以e得
$$e^2+xe-xe^2=0\cdot e=0$$
即$e+xe-xe=0$

从而得$e=0$。这与假设矛盾。因此$y\neq e$。于是y就有右拟逆元，根据引理，y的右拟逆元就是$e+x-xe$，即
$$0=y\circ(e+x-xe)=y+e+x-xe-y(e+x-xe)$$
$$=y+e+x-xe-ye-yx+yxe$$
把此式两边右乘以e得
$$0=0\cdot e=ye+e+xe-ye-yxe+yxe=e.$$
这与对e的假设矛盾。所以e是A的右恒等元。

因此，A含有恒等元$e=1$。

（2）设a是A中的任意非零元，$\because 1-a\neq 1$。
$\therefore$由假定，$1-a$有右拟逆元，记为$1-a'$。则
$$0=(1-a)(1-a')=1-a+1-a'-(1-a-a'+aa')=1-aa'$$
即$aa'=1$，a'是a的右逆元。显然$a'\neq 0$。

同样，$\because 1-a'\neq 1$，因此$1-a'$也有右拟逆元，由引理，这个右拟逆元就是$1-a$，即
$$0=(1-a')\circ(1-a)=1-a'a.$$
$\therefore a'a=1$，a'又是a的左逆元，$\therefore$a是A的单位元

由（1）（2）即知，A是除环。

〔证法二〕：必要性：设A是除环，$\therefore 1\in A$，显然1没有右拟元

若$a\in A$，$a\neq 1$，则$1-a\neq 0$，$(1-a)^{-1}\in A$。令$a'=1-(1-a)^{-1}$

则$a\circ a'=a\circ[1-(1-a)^{-1}]=a+1-(1-a)^{-1}-a+a(1-a)^{-1}=1+a(1-a)^{-1}-(1-a)^{-1}$

$$=1-(1-a)(1-a)^{-1}=1-1=0$$

∴a'是a的右拟逆元。

充分性：设e是环A唯一没有右拟逆元的元，显然$e\neq 0$，先证e是A的左恒等元。对任意$a\in A$必有$e\circ a=e$，若不然，$(e\circ a)$有右拟逆元b：$(e\circ a)\circ b=0$，即$e\circ(a\circ b)=0$。这说明A中存在元$a\circ b$是e的右拟逆元，与假设矛盾。于是由$e\circ a=e+a-ea=e$，得$ea=a$，即e是A的左恒等元。再证e是A唯一的左恒等元，设A还有左恒等元e'，则对任意$b\in A$，$e'b=b$，因而$e'\circ b=e'+b-e'b=e'+b-b=e'$。

如果$e'\neq e$，则必有$c\in A$，使得$e'\circ c=0$。

而$e'\circ c=e'$ ∴推得$e'=0$。这与e'是左恒等元的假设矛盾，

∴$e'=e$。即A只有唯一的左恒等元e。由习题23第6题知，e是A的双侧恒等元，记为1。

又，设a是A的任意非零元，∵$1-a\neq 1$，∴$1-a$有右拟逆元b：$(1-a)\circ b=1-a+b-b+ab=1-a+ab=0$

由此得$a(1-b)=1$。即$1-b$是a的右逆元，若c也是a的右逆元：$ac=1$，则因

$$(1-a)\circ(1-c)=1-a+1-c-1+a+c-ac$$
$$=1-ac=1-1=0$$

∴$1-c$是$1-a$的右拟逆元，由右拟逆元的唯一性知

$1-c=b$。即$c=1-b$。∴a的右逆元唯一，记为a^{-1}。

∵$a(a^{-1}+a^{-1}a-1)=1+a-a=1$。可见$a^{-1}+a^{-1}a-1$

是a的右逆元，∴$a^{-1}+a^{-1}a-1=a^{-1}$，即$a^{-1}a-1=0$．
$a^{-1}a=1$．
因此a^{-1}又是a的左逆元，∴a是A的单位元．

从而证得A是除环。

〔证法三〕：设$e\in A$，e没有右拟逆元，A的其余元都有右拟逆元．必要性与上法同，只就充分性另证．

（1）与证法（二）同，证明e是A的左恒等元

（2）由（1）证：e没有左拟逆元，A的其余元都有左拟逆元。事实上，若e有左拟逆元，则A中有a使得$a\circ e=0$即$a+e-ae=0$．两边右乘以得$aa^2+ea-aea=0$．
∵e是左恒等元，∴$ea=a$　即上述方程为$a^2-a-a^2=0$
∴$a=0$．由此得出$a\circ e=a+e-ae=e=0$，这与$e\neq 0$的假设矛盾，所以e没有左拟逆元．

又，设b是A的任意元，$b\neq e$，∵b有右拟逆元，∴存在$c\in A$使得$b\circ c=0$．∵e没有左拟逆元，∴$c\neq e$．因此c也有右拟逆元d：$c\circ d=0$．

∵$d=0\circ d=(b\circ c)\circ d=b\circ(c\circ d)=b\circ 0=b$．

∴$c\circ b=0$．

即任意非e的元b都有左拟逆元，它就是b的右拟逆元．

（3）由（2）证：e是A的右恒等元。首先，对任意$a\in A$必有$a\circ e=e$．若不然，$a\circ e$有左拟逆元b，$b\circ(a\circ e)=0$但$b\circ(a\circ e)=(b\circ a)\circ e=0$，于是得到e有左拟逆元$(b\circ a)$这与（2）中得到的结论矛盾。因此由$a\circ e=e$得到

$a+e-ae=e$．即$ae=a$．

∴e是右恒等元，因此e是双侧恒等元，记为1，

（4）A中任一$\neq 0$的元都是单位元，与证法一同．

习　题　25

1．计算

$$\begin{pmatrix} 1 & -2 & 3 \\ -2 & 1 & 3 \\ 0 & 1 & -1 \end{pmatrix}\begin{pmatrix} 3 & -5 & 6 \\ 7 & 2 & 1 \\ -1 & 1 & 2 \end{pmatrix}$$

〔解〕：原式 $=\begin{pmatrix} -14 & -6 & 10 \\ -2 & 15 & -5 \\ 8 & 1 & -1 \end{pmatrix}$

2．用例来验证I_2为非交换的，且含有$\neq 0$的零因子。

〔证〕：设I_2表示元素为整数的2阶矩阵的全体，如取

$$A=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\quad B=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\in I_2$$

$$AB=\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},\ \text{而}BA=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},\ \therefore AB\neq BA.$$

又取$C=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$，$D=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$是$I_2$的非零元，但

$$CD=DC=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$ ∴C，D是I_2的非零零因子。

3．如果$R\neq 0$，而$n>1$，求证：R_n有$\neq 0$的零因子。如果R含有元素a,b,使$ab\neq 0$．$n>1$，求证：R_n为非交换的。

〔证〕（1）∵$R\neq 0$，∴存在$a\in R$，$a\neq 0$．

取 $A=\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$，　$B=\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}\in R_n$

$A\neq 0$，$B\neq 0$，而$AB=BA=\begin{pmatrix}0&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}$ ∴A，B是

R_n的$\neq 0$的零因子。

（2）∵$ab\neq 0$，∴$a\neq 0$，$b\neq 0$

取 $C=\begin{pmatrix}a&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}$，$D=\begin{pmatrix}0&b&0&\cdots&0\\0&0&0&\cdots&0\\\vdots&\vdots&\vdots&&\vdots\\0&0&0&\cdots&0\end{pmatrix}\in R_n$

$CD=\begin{pmatrix}0&ab&0&\cdots&0\\0&0&0&\cdots&0\\\vdots&\vdots&\vdots&&\vdots\\0&0&0&\cdots&0\end{pmatrix}$ 而$DC=\begin{pmatrix}0&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}$

∴$CD\neq DC$。即R_n为非交换的。

习　题　26

1．求阵

$$\begin{pmatrix}-1&2&4\\3&2&0\\5&-1&2\end{pmatrix}$$

的伴随阵。

〔解〕：$\operatorname{adj}(a_{ij})=(A_{ji})=\begin{pmatrix}4&-8&-8\\-6&-22&12\\-13&9&-8\end{pmatrix}$

2．证明阵

$$(a)=\begin{pmatrix}1 & 4 & 1\\ 0 & 1 & -1\\ -3 & -6 & -8\end{pmatrix}$$

是I_3里的一个单位元素，这里I是整数环，并求这个阵的逆阵。

〔证〕：$\because \det(a)=\begin{vmatrix}1 & 4 & 1\\ 0 & 1 & -1\\ -3 & -6 & -8\end{vmatrix}=1$.

而1是整数环I的恒等元，当然是I的单位元，由§4定理1即知，(a)是I_3的单位元。这时(a)的逆矩阵即是它的伴随矩阵：

$$(a)^{-1}=\begin{pmatrix}-14 & 26 & -5\\ 3 & -5 & 1\\ 3 & -6 & 1\end{pmatrix}$$

3．如果R是带恒等元素的交换环，而(a)，$(b)\in R_n$求证：(a)(b)＝1可推得(b)(a)＝1

〔证〕：$\because (a)(b)=1$,

$\therefore \det[(a)(b)]=\det(a)\det(b)=1$.

又$\because$R是交换环，$\therefore \det(b)\det(a)=\det(a)\det(b)=1$

这就是说，det(b)是det(a)的逆元，$\therefore$det(a)是R的单位元．因此(a)是R_n的单位元，它有逆元$(a)^{-1}$：$(a)(a)^{-1}=(a)^{-1}(a)=1$

而$(a)^{-1}=(a)^{-1}[(a)(b)]=[(a)^{-1}(a)](b)=(b)$

$\therefore (b)(a)=(a)^{-1}(a)=1$.

习　题　27

1．计算$(-1+2i-3j+k)(2-i+3j-2k)$

〔解〕：原式 $= -2+4i-6j+2k+i+2+3ji-ki$

$-3j+6ij+9+3kj+2k-4ik+6jk+2$

$=11+5i-9j+4k+(-3k)(-j)+6k$

$-3i+4j+6i$

$=11+8i-6j+7k$。

2．我们定义 $a=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ 的迹 $T(a)=2\alpha_0$ 及距（或模方）$N(a)=\triangle=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$。验证a适合二次方程 $x^2-T(a)x+N(a)=0$。

〔证〕：$a^2=(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)^2=\alpha_0^2-\alpha_1^2$

$-\alpha_2^2-\alpha_3^2+2\alpha_0\alpha_1 i+2\alpha_0\alpha_2 j+2\alpha_0\alpha_3 k+$

$\alpha_1\alpha_2 ij+\alpha_1\alpha_2 ji+\alpha_1\alpha_3 ik+\alpha_1\alpha_3 ki+\alpha_2\alpha_3 jk$

$+\alpha_2\alpha_3 kj$

$=\alpha_0^2-\alpha_1^2-\alpha_2^2-\alpha_3^2+2\alpha_0\alpha_1 i+2\alpha_0\alpha_2 j$

$+2\alpha_0\alpha_3 k$

$T(a)a=2\alpha_0(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)=2\alpha_0^2+$

$2\alpha_0\alpha_1 i+2\alpha_0\alpha_2 j+2\alpha_0\alpha_3 k$

$N(a)=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$

$\therefore a^2-T(a)a+N(a)=(\alpha_0^2-\alpha_1^2-\alpha_2^2-\alpha_3^2+2\alpha_0$

$\alpha_1 i+2\alpha_0\alpha_2 j+2\alpha_0\alpha_3 k)-(2\alpha_0^2+2\alpha_0\alpha_1 i$

$+2\alpha_0\alpha_2 j+2\alpha_0\alpha_3 k)+\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2=0$。

即a满足方程 $x^2-T(a)x+N(a)=0$

3．求证：$N(ab)=N(a)N(b)$

〔证法一〕：设 $a=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$

$b=\beta_0+\beta_1 i+\beta_2 j+\beta_3 k$

则 $ab=(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)+(\alpha_0\beta_1+\alpha_1$

$\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)i+(\alpha_0\beta_2-\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3$

$\beta_1)j+(\alpha_0\beta_3+\alpha_1\beta_2-\alpha_1\beta_1+\alpha_3\beta_0)k$

$\therefore N(ab)=(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)^2+(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)^2+(\alpha_0\beta_2-\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3\beta_1)^2+(\alpha_0\beta_3+\alpha_1\beta_2-\alpha_1\beta_1+\alpha_3\beta_0)^2$

$=(\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2)(\beta_0^2+\beta_1^2+\beta_2^2+\beta_3^2)$

$=N(a)N(b)$

〔证法二〕令

$$(a)=\begin{pmatrix}\alpha_0+\alpha_1\sqrt{-1} & \alpha_2+\alpha_3\sqrt{-1}\\ -\alpha_2+\alpha_3\sqrt{-1} & \alpha_0-\alpha_1\sqrt{-1}\end{pmatrix}$$

$$(b)=\begin{pmatrix}\beta_0+\beta_1\sqrt{-1} & \beta_2+\beta_3\sqrt{-1}\\ -\beta_2+\beta_3\sqrt{-1} & \beta_0-\beta_1\sqrt{-1}\end{pmatrix}$$

$\because \det(a)=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2=N(a)$

$\det(b)=\beta_0^2+\beta_1^2+\beta_2^2+\beta_3^2=N(b)$

$N(ab)=\det(ab)$而$\det(ab)=\det(a)\det(b)$

$\therefore N(ab)=N(a)N(b)$

4．设α_i是有理数，求证：四维数$\alpha_0+\alpha_1i+\alpha_2j+\alpha_3k$的集合$Q_0$是Q的一个除子环，亦即$Q_0$是一个子环，并且是除环。

〔证〕：任取Q_0的二个元：

$$a=\alpha_0+\alpha_1i+\alpha_2j+\alpha_3k$$
$$b=\beta_0+\beta_1i+\beta_2j+\beta_3k$$

$a-b=(\alpha_0-\beta_0)+(\alpha_1-\beta_1)i+(\alpha_2-\beta_2)j+(\alpha_3-\beta_3)k.$

$\because \alpha_i$，β_i是有理数，$\therefore \alpha_i-\beta_i$也是有理数，（$i=0$，1，2，3）

$\therefore a-b\in Q_0$。所以Q_0对加法成群。

设$a=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k\neq 0$，则

$$N(a)=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2\neq 0$$

取$c=\frac{\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k}{\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2}$，c是a的逆元：

$ac=ca=1$。　　记$c=a^{-1}$。

$$ba^{-1}=(\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)\cdot\left(\frac{\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k}{\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2}\right)$$

$$=\frac{1}{\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2}\Big[(\beta_0\alpha_0+\beta_1\alpha_1+\beta_2\alpha_2+\beta_3\alpha_3)$$
$$+(-\beta_0\alpha_1+\beta_1\alpha_0-\beta_2\alpha_3+\beta_3\alpha_2)i+(-\beta_0\alpha_2$$
$$+\beta_1\alpha_3+\beta_2\alpha_0-\beta_3\alpha_1)j$$
$$+(-\beta_0\alpha_3-\beta_1\alpha_2+\beta_2\alpha_1+\beta_3\alpha_0)k\Big]$$

∵有理数经过加、减、乘、除的运算仍是有理数

∴$ba^{-1}\in Q$。即Q_0的非零元对于乘法成子群。

从而证得Q_0是Q的一个除子环。

5．如果α_i或者都是整数，或者都是奇整数的½，验证：四维数$\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$的集合J是Q的一个子环。J是否一个除环呢？

〔证法一〕任取$a=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$，

$$b=\beta_0+\beta_1 i+\beta_2 j+\beta_3 k\in J.$$

$$a-b=(\alpha_0-\beta_0)+(\alpha_1-\beta_1)i+(\alpha_2-\beta_2)j$$
$$+(\alpha_3-\beta^3)k.$$

1）当α_i，β_i都是整数，或α_i，β_i都是奇整数的½时，$(\alpha_i-\beta_i)$都是整数，（$i=0，1，2，3$）

2）当α_i（或β_i）都是整数，而β_i（或α_i）都是奇整数的½，则$(\alpha_i-\beta_i)$都是奇整数的½，($i=0，1，2，3$)

$\therefore a-b\in J$. 即J关于加法成子群。

又，$ab=(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)+(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)i+(\alpha_0\beta_2-\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3\beta_1)j+(\alpha_0\beta_3+\alpha_1\beta_2-\alpha_2\beta_1+\alpha_3\beta_0)k$

$\overset{记}{=}\gamma_0+\gamma_1 i+\gamma_2 j+\gamma_3 k$…………（*）

1）当α_i，β_i都是整数时，因为整数加减乘结果仍然是整数，$\therefore\gamma_i$都是整数，（$i=0,1,2,3$）

2）当α_i,β_i都是奇整数的½时，可令

$\alpha_i=\dfrac{2n_i+1}{2}$，$\beta_j=\dfrac{2m_j+1}{2}$，（$n_i,m_j$为整数）$\alpha_i\beta_j=\frac{1}{4}(2n_i+1)(2m_j+1)$，任一个$\gamma_k(k=0,1,2,3)$表为4个形如$\pm\frac{1}{4}(2n_i+1)(2m_j+1)$的和，即形为$\dfrac{偶数}{4}\pm\dfrac{偶数}{4}=\dfrac{整数}{2}$，所以$\gamma_k$可能是整数，也可能是奇数的½。但我们断言，$\gamma_k$要么全部是整数，要么全部是奇数的½。事实上，考虑$N(a)=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$，当$\alpha_i$都是整数时，$N(a)$当然是整数，当$\alpha_i$都是奇数的½时，可令$\alpha_i=\dfrac{2n_i+1}{2}$，则$\alpha_i^2=\dfrac{4n_i^2+4n_i+1}{4}\overset{令}{=}\dfrac{4m_i+1}{4}$（$m_i$为整数）此时。

$$N(a)=\sum_{i=0}^{3}\alpha_i^2=\sum\frac{4m_i+1}{4}=整数,$$

同理，不论β_i全是整数或全是奇数的½，$N(b)=\beta_0^2+\beta_1^2+\beta_2^2+\beta_3^2$，也是整数，$\therefore N(ab)=N(a)N(b)=\gamma_0^2+\gamma_1^2+\gamma_2^2+\gamma_3^2$是整数，如果$\gamma_i$（$i=0,1,2,3$）中

有一部分是整数，有一部分是奇数的½，则不可能保证 $\gamma_0^2+\gamma_1^2+\gamma_2^2+\gamma_3^2$ 是整数，所以 γ_i 要么全是整数，要么全是奇数的½，即 $a\cdot b\in J$.

3）当 α_i 都是整数，而 β_i 都是奇数的½，则 $\alpha_i\beta_i$ 是整数的½，而每个 γ_k 是4个 $\frac{整数}{2}$ 的代数和，所以 γ_k 可能是整数，也可能是奇数的½。与2）的证法同，为保证 $N(ab)=\gamma_0^2+\gamma_1^2+\gamma_2^2+\gamma_3^2$ 是整数，γ_k 必须全部是整数或全部是奇数的½。

当 β_i 全是整数，而 α_i 全是奇数的½，亦有同样的结果。

综合1），2），3），$ab\in J$，J关于乘法封闭．因此J构成Q的一个子环。

但J不是除环，如 $a=1+i+j+k\in J$，但 $a^{-1}=\frac{1}{4}(1-i-j-k)\overline{\in}J$.

〔证法二〕：只就 $a\in J$，$b\in J$，$\Rightarrow ab\in J$ 另法证明。

在上面式（＊）中，令 $(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)=d$，则

$$ab=d+[d+\alpha_0(\beta_1-\beta_0)+\alpha_1(\beta_0-\beta_1)+\alpha_2(\beta_3+\beta_2)+\alpha_3(\beta_3-\beta_2)]i+[d+\alpha_0(\beta_2-\beta_0)+\alpha_2(\beta_0+\beta_2)+\alpha_3(\beta_1+\beta_3)+\alpha_1(\beta_1-\beta_3)]j+[d+\alpha_0(\beta_3-\beta_0)+\alpha_3(\beta_0+\beta_3)+\alpha_1(\beta_2+\beta_1)+\alpha_2(\beta_2-\beta_1)]k$$

$$=d+[d+(\alpha_0+\alpha_1)(\beta_1-\beta_0)+(\alpha_2+\alpha_3)(\beta_3-\beta_2)+2(\alpha_1\beta_0+\alpha_2\beta_2)]i+[d+(\alpha_0+\alpha_2)(\beta_2-\beta_0)+(\alpha_3+\alpha_1)(\beta_1-\beta_3)+2(\alpha_0\beta_0+\alpha_3\beta_3)]j+[d+(\alpha_0+\alpha_3)(\beta_3-\beta_0)+(\alpha_1+\alpha_2)(\beta_2-\beta_1)+2$$

$(\alpha_3\beta_3+\alpha_1\beta_1)]k$

记 $d+(d+c_1)i+(d+c_2)j+(d+c_3)k$.

1）当 $\alpha_i\beta_i$ 都是整数时，显然，d 及 $d+c_i(i=1,2,3)$ 都是整数，$\therefore ab\in J$.

2）当 α_i，β_i 都是奇数的½，则.

$\alpha_0+\alpha_1$，$\beta_1-\beta_0$，$\alpha_2+\alpha_3$，$\beta_3-\beta_2$ 都是偶数的½，即为整数而 $2(\alpha_1\beta_0+\alpha_2\beta_2)=2\left(\frac{奇数}{4}+\frac{奇数}{4}\right)$

$=2\cdot\frac{偶数}{4}=\frac{偶数}{2}=整数$

$\therefore c_1=(\alpha_0+\alpha_1)(\beta_1-\beta_0)+(\alpha_2+\alpha_3)(\beta_3-\beta_2)+2(\alpha_1\beta_0+\alpha_2\beta_2)$ 是整数同样，C_2C_3 也都是整数。

$\because d=\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3=\frac{1}{4}$（奇数－奇数－奇数－奇数）$=\frac{1}{4}$偶数$=\frac{1}{2}$整数＝整数或奇数的½.

$\therefore$ 若 d 为整数，则 $d, d+c_1, d+c_2, d+c_3$ 也都是整数，若 d 为奇数的½，则，$d, d+c_1, d+c_2, d+c_3$ 也都为奇数的½.

$\therefore ab\in J$.

3）当 α_i（或 β_i）都是整数，而 β_i（或 α_i）都是奇数的½时.

则 $\alpha_0+\alpha_1$，$\beta_1-\beta_0$，$\alpha_2+\alpha_3$，$\beta_3-\beta_2$ 都是整数，

$$2(\alpha_1\beta_0+\alpha_2\beta_2)=2\left(\frac{整数}{2}+\frac{整数}{2}\right)=整数,$$

$\therefore c_1$ 是整数。同样，C_2, C_3 也都是整数.

$\because d=\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3$

$$=\frac{整数}{2}-\frac{整数}{2}-\frac{整数}{2}-\frac{整数}{2}=\frac{1}{2}整数=整数或奇数的\frac{1}{2}$$

∴当d为整数时，$d, d+c_1, d+c_2, d+c_3$都是整数，当d为奇数的½时，$d, d+c_1, d+c_2, d+c_3$都是奇数的½。

∴$ab\in J$。

习　题　28

1. 决定四维数环的心。

〔解〕设Q是四维数环，$C(Q)$是四维数环Q的心。

若$c=c_0+c_1i+c_2j+c_3k\in C(Q)$，必须而且只须对于任意$a=a_0+a_1i+a_2j+a_3k\in Q$，有

$$ca=ac.$$

即必须且只须

$$\begin{cases}\alpha_0c_0-\alpha_1c_1-\alpha_2c_2-\alpha_3c_3=c_0\alpha_0-c_1\alpha_1-c_2\alpha_2-c_3\alpha_3\\ \alpha_0c_1+\alpha_1c_0+\alpha_2c_3-\alpha_3c_2=c_0\alpha_1+c_1\alpha_0+c_2\alpha_3-c_3\alpha_2\\ \alpha_0c_2-\alpha_1c_3+\alpha_2c_0+\alpha_3c_1=c_0\alpha_2-c_1\alpha_3+c_2\alpha_0+c_3\alpha_1\\ \alpha_0c_3+\alpha_1c_2-\alpha_2c_1+\alpha_3c_0=c_0\alpha_3+c_1\alpha_2-c_2\alpha_1+c_3\alpha_0\end{cases}$$

$$即\begin{cases}\alpha_2c_3-\alpha_3c_2=0\\ \alpha_3c_1-\alpha_1c_3=0\\ \alpha_1c_2-\alpha_2c_1=0\end{cases}$$

由于α_i是任意的，要使上式成立，必须且只须$c_1=c_2=c_3=0$

∴$c(Q)=\{c_0 \mid c_0是实数\}$.

2. 令

$$(\alpha)=\begin{pmatrix}\alpha_1 & & 0\\ & \alpha_2 & \\ & & \ddots \\ 0 & & \alpha_n\end{pmatrix}$$

里的α_i是不同的有理数，R_0是有理数域．求证：阵环R_{0n}里的$C(\alpha)$是对角阵的集合，亦即是与(α)形状相同的阵的集合。

〔证〕：令 $(c)=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}$ 是R_{0n}的任一元，

若$(c)\in C(\alpha)$，必须且只须$(c)(\alpha)=(\alpha)(c)$

$$\because (c)(\alpha)=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}\begin{pmatrix} \alpha_1 & & & 0 \\ & \alpha_2 & & \\ & & \ddots & \\ 0 & & & \alpha_n \end{pmatrix}$$

$$=\begin{pmatrix} \alpha_1 c_{11} & \alpha_2 c_{12} & \cdots & \alpha_n c_{1n} \\ \alpha_1 c_{21} & \alpha_2 c_{22} & \cdots & \alpha_n c_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_1 c_{n1} & \alpha_2 c_{n2} & \cdots & \alpha_n c_{nn} \end{pmatrix}$$

$$(\alpha)(c)=\begin{pmatrix} \alpha_1 & & & 0 \\ & \alpha_2 & & \\ & & \ddots & \\ 0 & & & \alpha_n \end{pmatrix}\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}$$

$$=\begin{pmatrix} \alpha_1 c_{11} & \alpha_1 c_{12} & \cdots & \alpha_1 c_{1n} \\ \alpha_2 c_{21} & \alpha_2 c_{22} & \cdots & \alpha_2 c_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_n c_{n1} & \alpha_n c_{n2} & \cdots & \alpha_n c_{nn} \end{pmatrix}$$

比较两个矩阵的(i, j)元素知

$$\alpha_j c_{ij}=\alpha_i c_{ij}$$

即　　$(\alpha_i-\alpha_j)c_{ij}=0$

由假设，当$i\neq j$时，$a_i\neq a_j$，$\therefore a_i-a_j\neq 0$

因此必须，$c_{ij}=0$，即矩阵(c)除了对角线元素外，其余全为0，反之，若b是任一对角阵：

$$(b)=\begin{pmatrix}\beta_1\cdots 0\\ \cdots\\ 0\cdots\beta_n\end{pmatrix}，则$$

$$(\alpha)(b)=(b)(\alpha)$$

$$=\begin{pmatrix}\alpha_1\beta_1\cdots 0\\ \cdots\\ 0\cdots\ \alpha_n\beta_n\end{pmatrix}$$

故证得c(α)是对角阵的集合。

3.求证：R_{on}的心是纯量阵

$$\begin{pmatrix}\alpha & & 0\\ & \alpha & \\ & & \cdots\\ 0 & & \alpha\end{pmatrix}$$

的集合。

〔证〕设$(c)\in c(R_{on})$，(c)首先要与对角阵可交换由上题知，(c)必须是对角阵。$(c)=\begin{pmatrix}c_1 & & 0\\ & c_2 & \\ & & \cdots\\ 0 & & c_n\end{pmatrix}$

对任意$(a)\in R_{on}$，(c)还要满足$(c)(a)=(a)(c)$

$$(c)(a)=(c_ja_{ij})，\ (a)(c)=(a_{ij}c_i)$$

因此$c_ja_{ij}=a_{ij}c_i$即$(c_i-c_j)a_{ij}=0$

∵a_{ij}是任意的，∴$c_i - c_j = 0$，即$c_i = c_j$ 。

$$\therefore c = \begin{pmatrix} c & \cdots & 0 \\ & c & \\ & & \cdots \\ 0 & \cdots & c \end{pmatrix}$$

反之，若b是任一纯量阵：$(b) = \begin{pmatrix} \beta & \cdots & 0 \\ & \cdots & \\ 0 & \cdots & \beta \end{pmatrix}$，则对任一

$a = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in R_{on}$，有$(b)(a) = (a)(b) =$

$$\begin{pmatrix} \beta a_{11} & \cdots & \beta a_{1n} \\ \vdots & & \vdots \\ \beta a_{n1} & \cdots & \beta a_{nn} \end{pmatrix}$$

故证得$c(R_{on})$是纯量阵的集合。

4. 设 s 是I_2里如$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$形状的阵的集合，求c(s)

〔解〕设$(a) \in c(s)$，(α)与形如$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$的矩阵可交换当然与形如$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$的矩阵可交换，由第 2 题知$(\alpha)$为对角阵

可令$\alpha = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$。

$$\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} \alpha_1 a & \alpha_1 b \\ 0 & \alpha_2 c \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 a & \alpha_2 b \\ 0 & \alpha_2 c \end{pmatrix}$$

由 $\begin{pmatrix} \alpha_1 a & \alpha_1 b \\ 0 & \alpha_2 c \end{pmatrix} = \begin{pmatrix} \alpha_1 a & \alpha_2 b \\ 0 & \alpha_2 c \end{pmatrix}$ 得

$$\alpha_1 b = \alpha_2 b,\ 即(\alpha_1 - \alpha_2)b = 0$$

∵b是任意的，∴$\alpha_1 = \alpha_2 = \alpha$

∴$\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$

反之，由上题纯量矩阵当然与s里的矩阵可换即c(s)是I_2中纯量阵的集合。

习 题 29

1.如果n是整数，求证：na形的元素集合nA是一个理想。

〔证〕：令nA = {na|n是整数，a∈环A}，显然nA是A的子集，任取na，ma∈nA，则

na - ma = (n - m)a∈nA（∵n - m仍是整数）

∴nA，+是A的加法群的子群。

又，对任意b∈A，b·(na) = n(ba)∈nA（∵ba∈A）

且(na)b = n(ab)∈nA（∵ab∈A）

故nA是A的一个理想。

2.求证：在任一个环A里，使na = 0的元素a的集合N是一个理想。

〔证〕：令N = {a|na = 0，a∈A}，N当然是环A的子集，任取a_1，a_2∈N，则$na_1 = 0$，$na_2 = 0$

$n(a_1 - a_2) = na_1 - na_2 = 0 - 0 = 0$

∴$a_1 - a_2 \in N$

∴N，+是A的加法群的子群。

又，对任意$b\in A$。

$n(ba)=b(na)=b\cdot 0=0$，$\therefore ba\in N$。

且$n(ab)=(na)\cdot b=0\cdot b=0$，$\therefore ab\in N$。

故N是A的一个理想。

习　题　30

1. 如果D是含有q个元素的有限除环，求证：对于每个$a\in D$，

$$a^q=a$$

〔证〕：因为D是除环，所以D中非零元素集合G关于乘法构成一个群，因D的元数为q所以G的元数为$q-1$即G为$q-1$阶的群。由第一章Lagrange定理的推论，对于G中任意元a，有$a^{q-1}=1$，即$a^q=a$。

而对元0亦有$0^q=0$

$\therefore$对任意$a\in D$，恒有$a^q=a$。

习　题　31

1. 验证：对应$\alpha+\beta\sqrt{-1}\to\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}$是复数域C到$R_2$内的一个同构。

〔证〕：令$C=\{\alpha+\beta\sqrt{-1}\mid\alpha,\beta$为实数$\}$C是可换除环。

$$R_2=\left\{\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}\middle|\ \alpha,\beta\text{为实数}\right\}，R_2\text{是}$$

可换环。

设η：$\alpha+\beta\sqrt{-1}\to\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}$，若$\alpha_1+\beta_1\sqrt{-1}$

$=\alpha_2+\beta_2\sqrt{-1}$，则$\alpha_1=\alpha_2$，$\beta_1=\beta_2$ $\therefore\begin{pmatrix}\alpha_1 & \beta_1\\ -\beta_1 & \alpha_1\end{pmatrix}$

$=\begin{pmatrix}\alpha_2 & \beta_2\\ -\beta_2 & \alpha_2\end{pmatrix}$，反之，若$\alpha_1+\beta_1\sqrt{-1}\neq\alpha_2+\beta_2\sqrt{-1}$

则α_1与α_2，β_1与β_2中至少有一个不相等。

$\therefore\begin{pmatrix}\alpha_1 & \beta_1\\ -\beta_1 & \alpha_1\end{pmatrix}\neq\begin{pmatrix}\alpha_2 & \beta_2\\ -\beta_2 & \alpha_2\end{pmatrix}$ $\therefore\eta$是C到R_2内的

1－1映照，又显然

$$[(\alpha_1+\beta_1\sqrt{-1})+(\alpha_2+\beta_2\sqrt{-1})]\eta=$$

$$(\alpha_1+\beta_1\sqrt{-1})\eta+(\alpha_2+\beta_2\sqrt{-1})\eta$$

$$[(\alpha_1+\beta_1\sqrt{-1})\cdot(\alpha_2+\beta_2\sqrt{-1})]\eta$$

$$=(\alpha_1+\beta_1\sqrt{-1})\eta\cdot(\alpha_2+\beta_2\sqrt{-1})\eta$$

$\therefore\eta$是C到R内的一个同构。

2. 验证：对应$a=\alpha+\beta\sqrt{-1}\to\bar{a}=\alpha-\beta\sqrt{-1}$是C里一个自同构。

〔证〕：令：η：$a=\alpha+\beta\sqrt{-1}\to\bar{a}=\alpha-\beta\sqrt{-1}$，$\eta$把一个复数变为共轭复数，因为复数与其共轭复数是1－1对应，所以η是复数域C到自身上的1－1映照。又因

$[(\alpha_1+\beta_1\sqrt{-1})+(\alpha_2+\beta_2\sqrt{-1})]\eta=[(\alpha_1+\alpha_2)+(\beta_1+\beta_2)\sqrt{-1}]\eta=(\alpha_1+\alpha_2)-(\beta_1+\beta_2)\sqrt{-1}$
$=(\alpha_1-\beta_1\sqrt{-1})+(\alpha_2-\beta_2\sqrt{-1})=(\alpha_1+\beta_1\sqrt{-1})\eta+(\alpha_2+\beta_2\sqrt{-1})\eta$

而且，$[(\alpha_1+\beta_1\sqrt{-1})(\alpha_2+\beta_2\sqrt{-1})]\eta=[(\alpha_1\alpha_2-$

$\beta_1\beta_2)+(\alpha_1\beta_2+\alpha_2\beta_1)\sqrt{-1}]\eta$
$=(\alpha_1\alpha_2-\beta_1\beta_2)-(\alpha_1\beta_2+\alpha_2\beta_1)\sqrt{-1}=(\alpha_1-\beta_1\sqrt{-1})(\alpha_2-\beta_2\sqrt{-1})=(\alpha_1+\beta_1\sqrt{-1})\eta\cdot(\alpha_2+\beta_2\sqrt{-1})\eta$

∴η是C里的一个自同构。

3. 验证：对应 $\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\to\alpha$ 是对角阵环到它的系数环K内的一个同态。

〔证〕：令η：$\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\to\alpha$，∵若 $\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}=\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}$，则 $\alpha_1=\alpha_2=\alpha$，$\beta_1=\beta_2=\beta$，∴ $\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}\eta=\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}\eta=\alpha$ 所以η是单值映射，又因

$$\left[\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}+\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}\right]\eta=\begin{pmatrix}\alpha_1+\alpha_2 & 0\\ 0 & \beta_1+\beta_2\end{pmatrix}\eta=\alpha_1+\alpha_2=\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}\eta+\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}\eta$$

而且 $\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}\eta=\begin{pmatrix}\alpha_1\alpha_2 & 0\\ 0 & \beta_1\beta_2\end{pmatrix}\eta=\alpha_1\alpha_2=\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}\eta\cdot\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}\eta$

所以η是一个同态。

4. 验证：对应η：

$$\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k \to \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ -\alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2 \\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1 \\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}$$

是Q到R_4内的一个同构。

〔证〕：因为Q中任二个四维数相等，必须且只须四个分量对应相等，同样R_4中二个矩阵相等必须且只须对应元素相等。因此η显然是Q到R_4内的1－1映照。又因

$$[(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)+(\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)]\eta$$

$$=[(\alpha_0+\beta_0)+(\alpha_1+\beta_1)i+(\alpha_2+\beta_2)j+(\alpha_3+\beta_3)k]\eta$$

$$=\begin{pmatrix} (\alpha_0+\beta_0) & (\alpha_1+\beta_1) & (\alpha_2+\beta_2) & (\alpha_3+\beta_3) \\ -(\alpha_1+\beta_1) & (\alpha_0+\beta_0) & -(\alpha_3+\beta_3) & (\alpha_2+\beta_2) \\ -(\alpha_2+\beta_2) & (\alpha_3+\beta_3) & (\alpha_0+\beta_0) & -(\alpha_1+\beta_1) \\ -(\alpha_3+\beta_3) & -(\alpha_2+\beta_2) & (\alpha_1+\beta_1) & (\alpha_0+\beta_0) \end{pmatrix}$$

$$=\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ -\alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2 \\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1 \\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}+\begin{pmatrix} \beta_0 & \beta_1 & \beta_2 & \beta_3 \\ -\beta_1 & \beta_0 & -\beta_3 & \beta_2 \\ -\beta_2 & \beta_3 & \beta_0 & -\beta_1 \\ -\beta_3 & -\beta_2 & \beta_1 & \beta_0 \end{pmatrix}$$

$$=(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)\eta+(\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)\eta$$

而且，$[(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)\cdot(\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)]\eta$

$$=[(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)+(\alpha_0\beta_1+\alpha_1\beta_0$$
$$+\alpha_2\beta_3-\alpha_3\beta_2)i+(\alpha_0\beta_2+\alpha_2\beta_0+\alpha_3\beta_1-\alpha_1\beta_3)i$$
$$+(\alpha_0\beta_3+\alpha_3\beta_0+\alpha_1\beta_2-\alpha_2\beta_1)k]\eta$$

$$
\begin{array}{l}
= \left(\begin{array}{l}
(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3) \quad (\alpha_0\beta_1+\alpha_1\beta_0+ \\
-(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_2\beta_2) \quad (\alpha_0\beta_0-\alpha_1\beta_1- \\
-(\alpha_0\beta_2+\alpha_2\beta_0+\alpha_3\beta_1-\alpha_1\beta_3) \quad (\alpha_0\beta_3+\alpha_3\beta_0+ \\
-(\alpha_0\beta_3+\alpha_3\beta_0+\alpha_1\beta_2-\alpha_2\beta_1)-(\alpha_0\beta_2+\alpha_2\beta_0+
\end{array}\right. \\
\alpha_2\beta_3-\alpha_3\beta_2) \quad (\alpha_0\beta_2+\alpha_2\beta_0+\alpha_3\beta_1\alpha-\alpha_1\beta_3) \\
\alpha_2\beta_2-\alpha_3\beta_3)-(\alpha_0\beta_3+\alpha_3\beta_0+\alpha_1\beta_2-\alpha_2\beta_1) \\
\alpha_1\beta_2-\alpha_2\beta_1) \quad (\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)- \\
\alpha_3\beta_1-\alpha_1\beta_3) \quad (\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2) \\
\left.\begin{array}{l}
(\alpha_0\beta_3+\alpha_3\beta_0+\alpha_1\beta_2-\alpha_2\beta_1) \\
(\alpha_0\beta_2+\alpha_2\beta_0+\alpha_3\beta_1-\alpha_1\beta_3) \\
(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2) \\
(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)
\end{array}\right)
\end{array}
$$

$$
= \begin{vmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ -\alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2 \\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1 \\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0 \end{vmatrix} \begin{vmatrix} \beta_0 & \beta_1 & \beta_2 & \beta_3 \\ -\beta_1 & \beta_0 & -\beta_3 & \beta_2 \\ -\beta_2 & \beta_3 & \beta_0 & -\beta_1 \\ -\beta_3 & -\beta_2 & \beta_1 & \beta_0 \end{vmatrix}
$$

$$
=(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)\eta\cdot(\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)\eta
$$

所以η是Q到R_4内的一个同构。

习 题 32

1.令$m=rs\in I$，验证：$(r)/(m)$是$I/(m)$里一个理想，并证：$I/(m)/(r)/(m)\cong I/(r)$

(证)：(1)任取$\bar{a}\in(r)/(m)$则$\bar{a}=a+(m)$，$a\in(r)\subseteq I$

$\therefore\bar{a}\in I/(m)$，即$(r)/(m)$是$I/(m)$的一个子集。

对于任意的$\bar{a}=a+(m)\in(r)/(m)$，$\bar{b}=b+(m)\in(r)/(m)$，其中令$a=n_1r$，$b=n_2r$，(n_1，n_2为整数)，则

$\bar{a}-\bar{b}=(a-b)+(m)=(n_1-n_2)r+(m)$

$\therefore \bar{a}-\bar{b}\in(r)/(m)$

所以(r)/(m)关于I/(m)中的加法构成子群。

又，任意的$\bar{c}=c+(m)\in I/(m)$

$\bar{a}\bar{c}=ac+(m)=(n_1c)r+(m)\in(r)/(m)$

$\bar{c}\bar{a}=ca+(m)=(n_1c)r+(m)\in(r)/(m)$

因此(r)/(m)是环I/(m)的一个理想。

(2)作I/(m)到I/(r)内的映照η：$a+(m)\to a+(r)$

若$a+(m)=b+(m)$，则$(a-b)+(m)=0+(m)$

$\therefore a-b\equiv 0\ (\mathrm{mod}\,m)$ $\because r\mid m$，$\therefore a-b\equiv 0\ (\mathrm{mod}\,r)$

$\therefore a+(r)=b+(r)$，这说明 是单值映照。

又，$\{[a+(m)]+[b+(m)]\}^\eta=[(a+b)+(m)]^\eta=$
$(a+b)+(r)=a+(r)+b+(r)=[a+(m)]^\eta+[b+(m)]^\eta$

而且，$\{[a+(m)][b+(m)]\}=[ab+(m)]=ab+(r)=$
$[a+(r)][b+(r)]=[a+(m)]^\eta\cdot[b+(m)]^\eta$

∴ 是I/(m)到I/(r)内的同态映照，又因对I/(r)中任一元a+(r)，在I/(m)中都有原象a+(m)，所以 是 到 上的同态映照，即I/(r)是I/(m)的同态象。

现证(r)/(m)是同态的核，I/(r)的零元是(r)

设$\overline{K}=kr+(m)\in(r)/(m)$，则

$\overline{K}^\eta=[kr+(m)]^\eta=kr+(r)=(r)$

反之，对$\bar{a}=a+(m)\in I/(m)$，若

$\bar{a}^\eta=[a+(m)]^\eta=(r)$，则因

$[a+(m)]^\eta=a+(r)$，所以必须$a\equiv 0\ (\mathrm{mod}\,r)$

即$a=kr$，$\therefore \bar{a}=kr+(m)\in(r)/(m)$

由此可见(r)/(m)是η的同态核。

根据同态基本定理即知$I/(m)/(r)/(m) \cong I/(r)$

2.试在形如$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$的阵所构成的$I_2$的子环里，决定理想；并由此决定同态象。

〔解〕：令 $S=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c\in I\right\}$

易证S是I_2的一个子环，S的子集合S'要构成理想'须满足

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=\begin{pmatrix} aa_{11}+ba_{21} & aa_{12}+ba_{22} \\ ca_{21} & ca_{22} \end{pmatrix}\in S$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}=\begin{pmatrix} aa_{11} & a_{11}b+a_{12}c \\ aa_{21} & a_{21}b+a_{22}c \end{pmatrix}\in S'$$

从而必须$ca_{21}=0$，$aa_{21}=0$

$\because a_{21}$是任意的，$\therefore a=c=0$

即$S'=\left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b\in I\right\}$是$I_2$的理想

I_2关于S'的差环 I_2/S'是I_2的一个同态象。

3.如果$a\to\bar{a}$是R到$\overline{R}$内的一个同态，求证：$(a_{ij})\to(\bar{a}_{ij})$是$R_n$到$\overline{R}_n$内的一个同态。

〔证〕：令η：$a\to\bar{a}$，是R到$\overline{R}$内的一个同态。

φ：$(a_{ij})\to(\bar{a}_{ij})$，显然是$R_n$到$\overline{R}_n$内的单值映照。

事实上，若$(a_{ij})=(b_{ij})$，则$a_{ij}=b_{ij}$

由于η是单值映射，$\therefore \bar{a}_{ij}=\bar{b}_{ij}$， 即$(\bar{a}_{ij})=(\bar{b}_{ij})$

又，$[(a_{ij})+(b_{ij})]\varphi=(a_{ij}+b_{ij})\varphi=(\overline{a_{ij}+b_{ij}})$

$= [(a_{ij}+b_{ij})\eta] = ((a_{ij})\eta + (b_{ij})\eta) = (\bar{a}_{ij}+\bar{b}_{ij})$

$= (\bar{a}_{ij}) + (\bar{b}_{ij}) = (a_{ij})\varphi + (b_{ij})\varphi$

$$[(a_{ij})(b_{ij})]\varphi = (\sum_k a_{ik}b_{kj})\varphi = (\overline{\sum_k a_{ik}b_{kj}})$$

$= [(\sum_k a_{ik}b_{kj})\eta] = [(\sum_k \bar{a}_{ik}\bar{b}_{kj})] = (\bar{a}_{ij})(\bar{b}_{ij})$

$= (a_{ij})\varphi \cdot (b_{ij})\varphi$

∴ φ是R_n到$\bar{R}_n$内的一个同态。

4.令η是A到它自身内的一个同态，验证：被η所固定，亦即使$a\eta=a$的A里元素成一个子环，如果A是一个除环，并且$A\eta \neq 0$，则固定元素的集合构成一个除环。

〔证〕：（1）令$S=\{a \mid a\eta=a,\ a\in A,\ \eta$是A里一个自同态$\}$对任意$a_1,\ a_2\in S$，$a_1\eta=a_1$，$a_2\eta=a_2$

∵$(a_1-a_2)\eta = a_1\eta - a_2\eta = a_1 - a_2$

∴$a_1-a_2\in S$

即S对A的加法构成群

又∵$(a_1a_2)\eta = (a_1\eta)(a_2\eta) = a_1a_2$

∴$a_1a_2\in S$，即S对A的乘法封闭

可以S构成A的一个子环。

（2）若A是除环，则A有恒等元1，因为$A\eta \neq 0$，所以A里的自同态η把恒等元变为恒等元，即$1\eta=1$，因此$1\in S$，设$a(\neq 0)\in S$：$a\eta=a$，∴有逆元a^{-1}

∵$1 = 1\eta = (aa^{-1})\eta = a\eta(a^{-1})\eta = a\cdot(a^{-1})\eta$

两边同左乘a^{-1}即得$a^{-1}=(a^{-1})\eta$，∴$a^{-1}\in S$所以S是A的一个除子环。

5.求证：I到它自身内仅有的同态是恒等映照及把每个

元素映到0的映照，并就有理数域证明同一结果。

〔证〕：（1）I的恒等映照及把I中的每个元都变成0的映照显然是I内的自同态。

设η是I内的任一自同态，若1η=0，则对I中任意元a，$a\eta=(a\cdot 1)\eta=a\eta\cdot 1\eta=a\eta\cdot 0=0$

所以η把I中每个元都映成0。

若$1\eta\neq 0$，则对任意$a\in I$，有$a\eta=(a\cdot 1)\eta=(a\eta)\cdot\eta$ 于是$a\eta(1-1\eta)=0$，因$a\eta\neq 0\therefore 1-1\eta=0$即$1\eta=1$。其次对任意$a\in I$，若$a>0$，

$$a\eta=(a\cdot 1)\eta=(\underbrace{1+1+\cdots 1}_{a个})\eta=a\cdot(1\eta)=a\cdot 1=a$$

若$a<0$，则$-a>0$，由$(-a)\eta=-(a\eta)$，

有$-a=-(a\eta)\therefore a=a\eta$

即η把I中每个元都映成自身，∴η是A的恒等映照。

（2）设R为有理数域，η是R内的任一自同态

若1η=0，则同样有aη=0，a是R中任意元，此时η是把R中所有元都映成0的自同态。

若$1\eta\neq 0$，由（1）知，对任意q，$p\in I$，有$q\eta=q$，$p\eta=p$，由$1\eta=1$有$(p^{-1}\eta)=(p\eta)^{-1}$，

任取$a\in R$，a可表成$a=\dfrac{q}{p}$ $(p,q\in I,(p,q)=1)$

$$a\eta=(\frac{q}{p})\eta=(qp^{-1})\eta=q\eta\cdot(p^{-1}\eta)$$

$$=q\cdot p^{-1}=\frac{q}{p}=a$$

此时η是把R中所有元都映成自身的自同态，即η是R的恒等映照。

6。令B是一个集合，并令η是B到环A上的1－1映照，求证：合成

$$a+b=(a\eta+b\eta)\eta^{-1},\quad ab=[(a\eta)(b\eta)]\eta^{-1}$$

把B变到与A同构的环，应用这结果证明：任一个具有恒等元的环也是关于下面合成的一个环：

$$a\oplus b=a+b-1,\quad a\odot b=a+b-ab$$

〔证〕：（1）先证B关于两种合成构成环。1）$\because a\eta, b\eta\in A$，A是环，$\therefore a\eta+b\eta\in A$，$a\eta\cdot b\eta\in A$，$\eta$是B到A上的1－1映照，所以逆映照$\eta^{-1}$存在，$a\eta+b\eta$，$a\eta\cdot b\eta$有在B中的原象，所以$(a\eta+b\eta)\eta^{-1}$，$(a\eta\cdot b\eta)\eta^{-1}\in B$，即$a+b\in B$，$ab\in B$，2）$(a+b)+c=(a\eta+b\eta)\eta^{-1}+c=[(a\eta+b\eta)\eta^{-1}\cdot\eta+c\eta]\eta^{-1}=[(a\eta+b\eta)+c\eta]\eta^{-1}=[a\eta+(b\eta+c\eta)]\eta^{-1}=[a\eta+(b\eta+c\eta)\eta^{-1}\cdot\eta]\eta^{-1}=[a\eta+(b+c)\eta]\eta^{-1}=a+(b+c)$，3）$0\eta^{-1}$在B中关于加法起恒等元的作用：$a+0\eta^{-1}=(a\eta+0\eta^{-1}\cdot\eta)\eta^{-1}=a\eta\eta^{-1}=a$，4）对于$a\in B$，有$(-a\eta)\eta^{-1}\in B$，使得

$$a+(-a\eta)\eta^{-1}=[a\eta+(-a\eta)\eta^{-1}\eta]\eta^{-1}=(a\eta-a\eta)\eta^{-1}=0\eta^{-1}$$

5）$a+b=(a\eta+b\eta)\eta^{-1}=(b\eta+a\eta)\eta^{-1}=b+a$

6）$(ab)\cdot c=[(a\eta\cdot b\eta)\eta^{-1}]c=[(a\eta\cdot b\eta)\eta^{-1}\cdot\eta][c\eta]\eta^{-1}=[(a\eta\cdot b\eta)(c\eta)]\eta^{-1}=[a\eta\cdot(b\eta\cdot c\eta)]\eta^{-1}=[a\eta\cdot(b\eta\cdot c\eta)\eta^{-1}\eta]\eta^{-1}=[a\eta\cdot(b\cdot c)\eta]\eta^{-1}=a(bc)$

7）$a(b+c)=a[(b\eta+c\eta)\eta^{-1}]=[a\eta\cdot(b\eta+c\eta)\eta^{-1}\eta]\eta^{-1}=[a\eta(b\eta+c\eta)]\eta^{-1}=(a\eta\cdot b\eta+a\eta\cdot c\eta)\eta^{-1}=[(a\eta b\eta)\eta^{-1}\cdot\eta+(a\eta c\eta)\eta^{-1}\eta]\eta^{-1}=[(ab)\eta+(ac)\eta]\eta^{-1}=ab+ac$

$(b+c)d=(b\eta+c\eta)\eta^{-1}\cdot d=\{[(b\eta+c\eta)\eta^{-1}\cdot\eta]\cdot[d\eta]\}\eta^{-1}=[(b\eta+c\eta)d\eta]\eta^{-1}=(b\eta\cdot d\eta+c\eta d\eta)\eta^{-1}=[(b\eta\cdot d\eta)\eta^{-1}\cdot\eta+(c\eta\cdot d\eta)\eta^{-1}\eta]\eta^{-1}$

$=[(bd)\eta+(cd)\eta]\eta^{-1}=bd+cd$

因此B，+，·构成环。

再证B与A同构，因η是B到A上的1－1映照，而且，

$(a+b)\eta=[(a\eta+b\eta)\eta^{-1}]\eta=a\eta+b\eta$

$(a\cdot b)\eta=[(a\eta\cdot b\eta)\eta^{-1}]\eta=a\eta\cdot b\eta$

∴η是B到A上的同构映照，所以环B与环A同构。

（2）设A是具有恒等元的环，把A看作集合，作集合A到环A的映照η：$a\to 1-a$，这个映照显然是1－1的，并且是到上的，因为环A中任一元b，总可表成$b=1-c$，（只要取$c=1-b$），于是b在集合A中都有原象c。

集合A中定义的两种合成可表成如上面（1）的形式：

$a\oplus b=a+b-1=1-[(1-a)+(1-b)]$
$=[(1-a)+(1-b)]\eta^{-1}=(a\eta+b\eta)\eta^{-1}$

$a\circ b=a+b-ab=1-(1-a)(1-b)=(1-a)(1-b)\eta^{-1}=[(a\eta)(b\eta)]\eta^{-1}$

于是由（1）所证知，集合A关于合成⊕，o成环，并且与环（A，+，·）同构。

习 题 33

1. 验证：如$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$形的阵的 集合，当a，b都$\in$ I时，是I_2的一个子环，它有一个左恒等元素，但无右恒等元素。于是，证明：这个环不与它自身成反同构。

〔证〕令 $S=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, \ b\in I\right\}$

（1）任取$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$，$\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}\in S$，则

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}-\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_1-a_2 & b_1-b_2 \\ 0 & 0 \end{pmatrix}\in S$$

∴S对于I_2中的加法构成子群

又$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_1b_2 & a_1b_2 \\ 0 & 0 \end{pmatrix}\in S$

（∵a_1a_2，$b_1b_2\in I$）

∴S对于I_2中的乘法构成子半群，因此S是I_2的子环。

（2）S 有一个左恒等元$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$：$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ $=\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$但无右恒等元，∵$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & b \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} ac & ab \\ 0 & 0 \end{pmatrix}$

要使$\begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$

必取$ac=a$，$ad=b$，即$c=1$，$d=\frac{b}{a}$

但因$d=\frac{b}{a}\overline{\in} I$，所以S中不存在阵 $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}$使得

$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$，即S中无右恒等元。

（3）设η：$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix}$是S到自身上任意一个1－1映照，因为

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right]\eta = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\eta = \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix}$$

但是 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\eta \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\eta = \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\eta$

由上面（2）知，S中没有右恒等元，∴ $\begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\eta$

$\neq \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix}$因此对任意$\eta$，都有

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right]\eta \neq \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\eta \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\eta$$，即反同构映照不存在，所以S不与它自身反同构。

2. 对于半群定义反同构，求证：任一个群都与它自身成反同构。

〔定义〕：设S_1，S_2是半群，若存在S_1到S_2上的一个1－1映照η，满足：对于任意的a，b∈S_1，都有，

$(ab)\eta = b\eta \cdot a\eta$

则称半群S_1，S_2为反同构。

〔证〕：设G是任一个群，作映照

η：$a \to a^{-1}$，$a \in G$

显然η到G自身上的1－1映照，而且

$(ab)\eta=(ab)^{-1}=b^{-1}a^{-1}=b\eta\cdot a\eta$

∴ η是G到自身上的反同构映照，即G与它自身成反同构。

3.一个环到它自身上的一个反同构叫做反自同构。求证：一个环的自同构及反自同构构成一个变换群。验证：在这个群里自同构构成指标为1或2的一个不变子群。

〔证〕：设A是环，令

$G=\{\eta_i,\ \eta_i' \mid \eta_i, \eta_i'$分别为A的自同构和反自同构$\}$

（1）因为环A的自同构与反同构都是A到自身上的1－1映照，所以它们的乘积也都是A到自身上的1－1映照，即G中元都是A上的1－1变换。现证G构成群。

1）满足封闭性：两个自同构的乘积仍是自同构，事实上，设η_i，η_j是A的两个自同构，则对于a，b∈A

$$(a+b)\eta_i\eta_j=[(a+b)\eta_i]\eta_j=(a\eta_i+b\eta_i)\eta_j$$
$$=a\eta_i\eta_j+b\eta_i\eta_j$$

$$(ab)\eta_i\eta_j=[(ab)\eta_i]\eta_j=[(a\eta_i)(b\eta_i)]\eta_j$$
$$=(a\eta_i)\eta_j\cdot(b\eta_i)\eta_j=a(\eta_i\eta_j)\cdot b(\eta_i\eta_j)$$

两个反同构的乘积是一个自同构。事实上，设η_i'，η_j'是两个反自同构，有

$$(a+b)\eta_i'\eta_j'=a(\eta_i'\eta_j')+b(\eta_i'\eta_j')$$

$$(ab)\eta_i'\eta_j'=[(b\eta_i')(a\eta_i')]\eta_j'=(a\eta_i')\eta_j'\cdot$$
$$(b\eta_i')\eta_j'=a(\eta_i'\eta_j')\cdot b(\eta_i'\eta_j')$$

一个自同构与一个反自同构的乘积是一个反自同构。事实上，设η_i是自同构，η_i'是反自同构，有

$$(a+b)\eta_i\eta_i'=a(\eta_i\eta_i')+b(\eta_i\eta_i')$$

$$(ab)\eta_i\eta_i'=[(a\eta_i)(b\eta_i)]\eta_i'=(b\eta_i)\eta_i'\cdot$$

$$(a\eta_i)\eta_i' = b(\eta_i\eta_i')\cdot a(\eta_i\eta_i')$$

同样 $$(a+b)\eta_i'\eta_i = a(\eta_i'\eta_i)+b(\eta_i'\eta_i)$$

$$(ab)\eta_i'\eta_i = b(\eta_i'\eta_i)\cdot a(\eta_i'\eta_i)$$

所以G中任意两个元的乘积仍是G中元。

2）满足结合律：G中元都是A上的1－1映照，而这些映照的乘积是满足结合律的。而且合成的结果是自同构还是反自同构并不因不同的结合而改变。

3）A上的恒等映照1是A的一个自同构，$\therefore 1\in G$，$1\cdot\eta_i=\eta_i\cdot 1=\eta_i$，$1\cdot\eta_j'=\eta_j'\cdot 1=\eta_j'$，$\therefore 1$是G的恒等元素。

4）η是自同构，则η^{-1}也是自同构，事实上

$$(a\eta^{-1}+b\eta^{-1})\eta=(a\eta^{-1})\eta+(b\eta^{-1})\eta=a+b$$

$$\therefore (a+b)\eta^{-1}=a\eta^{-1}+b\eta^{-1}$$

且 $$(a\eta^{-1}\cdot b\eta^{-1})\eta=(a\eta^{-1})\eta\cdot(b\eta^{-1})\eta=ab$$

$$\therefore (ab)\eta^{-1}=a\eta^{-1}\cdot b\eta^{-1}$$

η'是反自同构，则η'^{-1}也是反自同构。事实上，

$$(a\eta'^{-1}+b\eta'^{-1})\eta'=a+b$$

$$\therefore (a+b)\eta'^{-1}=a\eta'^{-1}+b\eta'^{-1}$$

且 $$[(b\eta'^{-1})(a\eta'^{-1})]\eta'=(a\eta'^{-1})\cdot(b\eta'^{-1})\eta'=ab$$

$$\therefore (ab)\eta'^{-1}=b\eta'^{-1}\cdot a\eta'^{-1}$$

因此，对于G中的任意元，G中都有它的逆元。从而证得G是A到自身上的变换群。

（2）令$G_1=\{\eta_i \mid \eta_i$是A的自同构$\}$

因为恒等映照$1\in G_1$，$\therefore G_1$是G的非空子集，又因

1）$\eta_i\eta_j=\eta_k\in G_1$，

2）1是G_1的单位元

3）$\eta_i^{-1}\in G_1$， 4）任取G中的元g，

若$g\in G_1$，则$g^{-1}\in G_1$，$\therefore g^{-1}\eta_i g\in G_1$

若$g\overline{\in} G_1$，则g是反自同构，g^{-1}也是反自同构，$g^{-1}\eta_i$是反自同构，$g^{-1}\eta_i g\in G_1$

由此可见G_1是G的不变子群。

当A是可换环时，则A的反自同构也都是自同构，因此$G=G_1$，此时G_1的指标就是1，当A是非可换环时，如果A没有反自同构，同样有$G=G_1$，G_1的指标也是1。如果A有反自同构a，则A的任一反自同构η'可表为$\eta'=a(a^{-1}\eta')$，a^{-1}是反自同构，$a^{-1}\eta'$是自同构，$\therefore a^{-1}\eta'\in G_1$，即$\eta'\in aG_1$，反之$aG_1$中任意元当然都是反同构，$\therefore G=G_1+aG_1$，此时$G_1$的指标就是2。

4.如果$a\to\bar{a}$是R到$\overline{R}$上的一个反同构，验证：映照$(a)\to(\bar{a})'$是R_n到$\overline{R}_n$上的一反同构，这里$(\bar{a})'$的(ij)元素是$\bar{a}_{ji}$

〔证〕：$\because a\to\bar{a}$是R到$\overline{R}$上的一个反同构，它是1－1映照，$\therefore (a)\to(\bar{a})'$显然是$R_n$到$\overline{R}_n$上的1－1映照。

$$\therefore (a_{ij})+(b_{ij})=(a_{ij}+b_{ij})\to(\overline{a_{ij}+b_{ij}})'=(\bar{a}_{ij}\bar{b}_{ij})'$$
$$=(\bar{a}_{ij})'+(\bar{b}_{ij})'$$

$$(a_{ij})(b_{ij})=(\Sigma a_{ik}b_{kj})\to(\overline{\Sigma a_{ik}b_{kj}})'=(\Sigma\bar{a}_{ik}+\bar{b}_{kj})'$$
$$=(\bar{b}_{ij})(\bar{a}_{ij})$$

$\therefore (a)\to(\bar{a})'$是$R_n$到$\overline{R}_n$上的一个反同构。

5.试定义反同态，说出并且证明对于反同态的基本定理。

〔定义〕：设η是环A到环A′内的一个映照，若对于A中的任意两个元a,b，有

$(a+b)\eta=a\eta+b\eta$

$$(ab)\eta = b\eta \cdot a\eta$$

则称η是环A到环A′内的一个**反同态**。

反同态基本定理：环A关于它的任一理想B的差环A/B必反同构于A的一个反同态象；反之，A的任一个反同态象必反同构于A的一个差环。

〔证〕：(1)对于差环(A/B, +·)，的集合A/B，定义二种合成法：加法+与原来相同，乘法×为

$$(a+B)\times(b+B) = ba+B$$

集合A/B关于乘法×的封闭性是显然的。又因为

$$[(a+B)\times(b+B)]\times(c+B) = (ba+B)\times(c+B) = cba+B$$

$$(a+B)\times[(b+B)\times(c+B)] = (a+B)\times(cb+B) = cba+B$$

∴关于×的结合律成立

$$[(a+B)+(b+B)]\times(c+B) = [(a+b)+B]\times(c+B)$$
$$= c(a+b)+B = (ca+B)+(cb+B)$$
$$= (a+B)\times(c+B)+(b+B)\times(c+B)$$

$$(d+B)\times[(a+B)+(b+B)] = (d+B)\times[(a+b)+B]$$
$$= (a+b)d+B = (ad+B)+(bd+B)$$
$$= (d+B)(a+B)+(d+B)(b+B)$$

∴关于×对+的分配律成立，从而(A/B, +, ×)是一个环而且(A/B, +, ·)与(A/B, +, ×)之间存在恒等映照φ，使得

$$[(a+B)+(b+B)]\varphi = (a+B)\varphi+(b+B)\varphi$$

$$[(a+B)\cdot(b+B)]\varphi = (ab+B)\varphi = (ab+B)$$
$$= (b+B)\times(a+B) = (b+B)\varphi\times(a+B)\varphi$$

因此(A/B, +, ·)与(A/B, +, ×)反同构。

现证(A/B, +, ×)是A的一个反同态象。

设υ：$a \to a+B$是A到(A/B, ×, +)内的一个映照，显然υ是单值映照，而且

$$(a+b)\upsilon=(a+b)+B=(a+B)+(b+B)=a\upsilon+b\upsilon$$

$$(ab)\upsilon=(ab+B)=(b+B)\times(a+B)=(b\upsilon)\times(a\upsilon)$$

∴υ是A到(A/B, +, ×)内的一个反同态（称为自然反同态）又因对于(A/B, +, ×)任一元$b+B$，A中都有元b与之对应，所以(A/B, +, ×)是A的一个反同态象。

综上所述，A/B反同构于A的一个反同态象。

(2)设η是A到A′上的一个反同态，A′是A的反同态象，令$K=\eta^{-1}(0)=\{a \mid a\eta=0, a\in A\}$

任取a, $b\in K$，则$a\eta=0$，$b\eta=0$

$$(a-b)\eta=a\eta-b\eta=0-0=0$$

∴$a-b\in K$，K对于A中的加法构成A的加法群的子群。

又，对任意的$c\in A$，$a\in K$

$$(ca)\eta=a\eta\cdot c\eta=0\cdot c\eta=0$$

$$(ac)\eta=c\eta\cdot a\eta=c\eta\cdot 0=0$$

∴K是A的一个理想。

现证差环A/K与A′反同构。

作A/K到A′内的映照$\overline{\eta}$：$a+K\to a\eta$，则$\overline{\eta}$是1－1的，且是到上的，事实上，若$a+K=b+K$，则$a\eta=(a+K)\overline{\eta}=(b+K)\overline{\eta}=b\eta$

反之，若$a\eta=b\eta$，则$a\eta-b\eta=(a-b)\eta=0$，∴$a-b\in K$

∴$a+K=[b+(a-b)]+K=b+K+(a-b)+K=b+K$而且对于任意的$c\eta\in A'$，都有$c+K\in A/K$与之对应，又因$\overline{\eta}$满足：

$$[(a+K)+(b+K)]\overline{\eta}=[(a+b)+K]\overline{\eta}=(a+b)\eta$$

$$a\eta+b\eta=(a+K)\overline{\eta}+(b+K)\overline{\eta}$$

$$[(a+K)(b+K)]\overline{\eta}=(ab+K)\overline{\eta}=ab\eta=b\eta a\eta$$

$$=(b+K)\overline{\eta}(a+K)\overline{\eta}$$

∴ η 是A/K到A′上的一个反同构，即A/K与A′反同构，这就是说，A的任一个反同态象必与A的一个差环反同构。

6.求证华罗庚定理：令s是环A到环B内的一个映照，使$(a+b)^s=a^s+b^s$，并且对每两个元素a，b，或者$(ab)^s=a^sb^s$者或$(ab)^s=b^sa^s$则s是一个同态，或者是一个反同态。

〔证〕：（1）先证对于映照s，若A中存在a，b使得

$$(ab)^s=a^sb^s$$

则对A中任意元a′，b′，恒有$(a'b')^s=a'^sb'^s$

1）若有a，b使得$(ab)^s=a^sb^s$，则对任意$c\in A$，也有

$$(ac)^s=a^sc^s$$

事实上，∵$(ab+ac)^s=(ab)^s+(ac)^s$

如果$(ac)^s=c^sa^s$，则$(ab+ac)^s=a^sb^s+c^sa^s$

但$(ab+ac)^s=[a(b+c)]^s$

如果$[a(b+c)]^s=a^s(b+c)^s=a^sb^s+a^sc^s$

则有$a^sb^s+c^sa^s=a^sb^s+a^sc^s$，于是有$c^sa^s=a^sc^s$，这是不可能的。

同样，如果$[a(b+c)]^s=(b+c)^sa^s=b^sa^s+c^sa^s$

则有$a^sb^s+c^sa^s=b^sa^s+c^sa^s$，于是有$a^sb^s=b^sa^s$，也是不可能的。

∴$(ac)^s=a^sc^s$

2）同理可证：若有a，b使得$(ab)^s=a^sb^s$，则对任意

的$d\in A$，也有$(db)^s=d^sb^s$

3）对于A中任意元a'，b'，A中必有c，d，使得

$$a'=a+c,\ b'=b+d$$

$$(a'b')^s=[(a+c)(b+d)]^s=(ab+cb+ad+cd)^s$$
$$=(ab)^s+(cb)^s+(ad)^s+(cd)^s$$

由2）知，若$(ab)^s=a^sb^s$，则$(cb)^s=c^sb^s$，$(ad)^s=a^sd^s$，$(cd)^s=c^sd^s$，所以此时有

$$(a'b')^s=a^sb^s+c^sb^s+a^sd^s+c^sd^s$$

而$a'^s\cdot b'^s=(a+c)^s\cdot(b+d)^s=(a^s+c^s)(b^s+d^s)$
$$=a^sb^s+c^sb^s+a^sd^s+c^sd^s$$

$$\therefore (a')^s(b')^s=(a'b')^s$$

（2）对于映照，若A中存在a，b，使$(ab)^s=b^sa^s$，则对任意的a'，$b'\in A$，亦有$(a'b')^s=b'^sa'^s$。若不然，必有c，$d\in A$，使得$(cd)^s=c^sd^s$，则根据（1）对于所有c'，$d'\in A$，亦有$(c'd')^s=c'^sd'^s$，于是$(ab)^s=a^sb^s$，这与假设矛盾。

因为s保持加法，所以当出现情况（1）时，s就是一个同态，当出现情况（2）时，s就是反同态。

习　　题　　34

1.验证：在定理7里用单纯环代替整区也能成立。

此题即要证：A是一个单纯环，若A的特征数为0，则A中任意非零元的阶数都是∞，若A的特征数$m>0$，则m是一个素数，并且A中所有非零元的阶数都是m。

〔证〕：（1）若A中存在一个元$a\neq 0$，其阶数为$m<\infty$，则$ma=0$，作集合$S=\{a\mid ma=0,\ a\in A\}$

任取a，b∈S，$ma=0$，$mb=0$

$m(a-b)=ma-mb=0-0=0$

对任意c∈A，$m(ca)=c(ma)=c\cdot 0=0$

$$m(ac)=(ma)c=0\cdot c=0$$

∴S是A的一个理想，因A是单纯环，所以S=0，或S=A，但因a（≠0）∈S，∴S=A

即对任意$a'\in A$，$ma'=0$，所以A的特征数为m，与A的特征数为0的假设矛盾，所以A的所有非零元都是无限阶。

（2）设A的特征数为$m>0$，则A中必存在$a\neq 0$，使得$ma=0$，而对于$m_1<m$，$m_1a\neq 0$且对任意的b（≠0）∈A，b的阶数≤m。

设b是A中的任意非零元，其阶数为m'，作集合

$S_1=\{s\mid m's=0\}$

与上面的证法相同，S_1是A的一个理想，并且$S_1=A$。因此，对于A中任意非零元a，有$m'a=0$，即a的阶数≤m'，由此可知$m'=m$，即A中所有非零元的阶数都是m。

现证m是素数，若不然，设$m=m_1m_2$，m_1，$m_2>1$，则对任意a（≠0）∈A

$0=ma=m_1m_2a=m_1(m_2a)$

∴元m_2a的阶数≤$m_1<m$

但a的阶数为m，∴$m_2a\neq 0$，所以m_2a的阶数也是m，这就得出矛盾，因此m是质数。

习　题　35

1.求证：不含有真左理想的环A或者是一个除环，或者

是一个零环。

〔证〕：若A是一个零环，它当然不含有真左理想。现假定A是一个不含有真左理想的非零环。

1）先证A是一个整区。为此，作集合

$H_a=\{x \mid xa=0,\ a\neq 0,\ a\in A\}$

任取x，$y\in H_a$，则 $(x-y)a=xa-ya=0-0=0$

$\therefore x-y\in H_a$，对任意的$b\in A$，$(bx)a=b(xa)=b\cdot 0=0$

$\therefore AH_a\subseteq H_a$，因而$H_a$是A的一个左理想，因为A不含有真左理想，$\therefore H_a=0$或$H_a=A$

再造集合$S=\{a_i \mid H_{a_i}=A\}$。任取a_i，$a_j\in S$，则对任意的$b\in A$，有$ba_i=0$，$ba_j=0$

$$b(a_i-a_j)=ba_i-ba_j=0-0=0$$

$\therefore a_i-a_j\in S$，又

$b(xa_i)=b\cdot 0=0$（x是A中任意元），$xa_i\in S$，$AS\subseteq S$

$\therefore$S也是A的一个左理想。

同样$S=0$或$S=A$

但若$S=A$，则对任意的$y\in A$，必有$y\in S$，$\therefore$对任意的$x\in A$，都有$xy=0$，于是A是零环，这与假设矛盾，$\therefore S=0$，所以只有$H_0=A$，这就是说，对于A中的任意元$b\neq 0$，只有0满足$b0=0$，换句话说，若$a\neq 0$，$b\neq 0$，则必有$ab\neq 0$，因此A是整区。

2）对任意$a(\neq 0)\in A$，Aa是A的左理想，且$Aa=A$，事实上，任取xa，$ya\in Aa$，$xa-ya=(x-y)a\in Aa$对任意的$c\in A$，$c(xa)=(cx)a\in Aa$，$\therefore$Aa是A的一个左

理想，则$Aa=0$或$Aa=A$，但因A是整区，$a\neq 0$，$\therefore aa\neq 0$，$aa\in Aa$，$\therefore Aa\neq 0$，因此$Aa=A$，由此可知，方程$xa=b\ (b\in A)$在A中有解。

3）设e是方程$xa=a$的解，要证e就是A的恒等元。为此，作集合$E_l=\{x\mid ex=x\}$，$E_r=\{y\mid ye=y\}$，任取$x\ (\neq 0)\in E_l$，$\because (xe-x)x=xex-x^2=x^2-x^2=0$，而A是整区，$\therefore xe-x=0$，$xe=x$

即$x\in E_r$，$\therefore E_l\subseteq E_r$

反之，任取$y\ (\neq 0)\in E_r$，$\because y(ey-y)=yey-y^2=y^2-y^2=0$，而A是整区，$\therefore ey-y=0$，即$ey=y$

即$y\in E_l$，$\therefore E_r\subseteq E_l$，因此$E_l=E_r$，这就说明对于集合$E_l$，$E_r$来说，e是左恒等元，又是右恒等元。

现证E_r是A的一个左理想，且$E_r=A$，这是因为，任取y_1，$y_2\in E_r$，$(y_1-y_2)e=y_1e-y_2e=y_1-y_2$

$\therefore y_1-y_2\in E_r$，又，对任意$c\in A$，$(cy)e=c(ye)=cy$

$\therefore AE_r\subseteq E_r$，因此$E_r$是A的一个左理想，从而$E_r=0$或$E_r=A$，但由集合$E_l$与$E_r$的构造知道，$E_r$含有非0元，$\therefore E_r=A$，因此e是A的左恒等元，又是A的右恒等元，即e是A的恒等元。

于是得到A是一个带有恒等元$\neq 0$，不拥有真左理想的环，由定理8即知，A是除环。

2.如果A是任一个环，则A^2，A^3，…，是理想。如果A是I_3里由形如

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

的阵所构成的子环，这些理想是什么？

〔证〕：$\because A^k=\left\{\sum_{i=1}^{n} a_{i_1}a_{i_2}\cdots a_{ik} \mid a_{ij}\in A,\ j=1,\ \cdots,\right.$ k，n为任意自然数$\}$

任取a，b∈A^k，则a－b显然仍是$\sum_{i=1}^{n} a_{i_1}a_{i_2}\cdots a_{ik}$的形式

$\therefore a-b\in A^k$，又，对任意的c∈A

$$c\left(\sum_{i=1}^{n} a_{i_1}a_{i_2}\cdots a_{ik}\right)=\sum_{i=1}^{n}(ca_{i_1})a_{i_2}\cdots a_{ik}\in A^k$$

同样，$\left(\sum_{i=1}^{n} a_{i_1}a_{i_2}\cdots a_{ik}\right)c=\sum_{i=1}^{n} a_{i_1}a_{i_2}\cdots(a_{ik}c)\in A^k$

$\therefore A^k$（k＝1，2，…）是A的理想。

若A为I_3里形如$\begin{pmatrix}0&a&b\\0&0&c\\0&0&0\end{pmatrix}$的阵所构成的子环，则A的形如$A^k$的理想为

$$A=\left\{\begin{pmatrix}0&a&b\\0&0&c\\0&0&0\end{pmatrix}\middle|\ a,\ b,\ c\in I\right\}$$

$$A^2=\left\{\begin{pmatrix}0&0&d\\0&0&0\\0&0&0\end{pmatrix}\middle|\ d\in I\right\}$$

$$A^k=\left\{\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}\right\}, k\geqslant 3$$

习 题 36

1.决定n阶循环群的自同态环及自同构群

〔解〕：设G是n阶循环群：$G=[a]$，$na=0$

$S\{\eta_i \mid \eta_i$是G的自同态$\}$

任取$\eta_k\in S$，$a\eta_k=ka$

对于G中任意元ma，$\because (ma)\eta_k=m(a\eta_k)=m(ka)=k(ma)$

$\therefore \eta_k$是由它对于生成a的作用效果所决定。

设$a\eta_i=ia$，作S到$I/(n)$内的映照φ：

$$\eta_i\to\bar{i}$$

当$\eta_i=\eta_j$时，则$a\eta_i=a\eta_j$，即$ia=ja$，$\therefore \bar{i}=\bar{j}$

反之，若$\bar{i}=\bar{j}$，则$i-j\equiv 0\ (\mathrm{mod}\,n)$，即$i-j=nn_1$

$\therefore ia-ja=(i-j)a=nn_1a=n_1(na)=n_1 0=0$

$\therefore ia=ja$，$\therefore \eta_i=\eta_j$，这就是说φ是S到$I/(n)$内的1－1映照，而且是到上的。事实上，对任意$\bar{k}\in I/(n)$，作映照η：$a\to ka$，这显然是G到G内的映照，而且

$$k(a+b)=ka+kb$$

$\therefore$它是G的一个自同态，$\therefore \eta\in S$

且$\eta\varphi=\bar{k}$，又因为

$a(\eta_i+\eta_j)=a\eta_i+a\eta_j=ia+ja=(i+j)a$

$\therefore (\eta_i+\eta_j)\varphi=\overline{i+j}=\bar{i}+\bar{j}=\eta_i\varphi+\eta_j\varphi$

$a(\eta_i\eta_j)=(a\eta_i)\eta_j=(ia)\eta_j=j(ia)=ija$

$\therefore (\eta_i \eta_j)\varphi = \overline{ij} = \overline{i}\,\overline{j} = (\eta_i\varphi)(\eta_j\varphi)$

$\therefore \varphi$是一个S到I/(n)上的同构。

即$S \cong I/(n)$

设$\eta_k \in S$，$a\eta_k = ka$

如果η_k是G的一个自同构，因为自同构把生成元变成生成元，∴ka是G的生成元，∴必须满足$(k, n) = 1$，即G的自同构全体构成$\varphi(n)$阶的群S′：

$$S' = \{\eta_k \mid a\eta_k = ka,\ a \in G,\ (k, n) = 1\}$$

2. 令G是一个任意群，并令M是G到它自身内的全部映照的集合。如果η，$\rho \in M$，定义$\eta\rho$是它们的积，而$\eta + \rho$为$g(\eta + \rho) = (g\eta)(g\rho)$，求考究关于这两个合成的集合M。

〔解〕：由已知中的定义可见，G的合成是用乘法表示。

令$M = \{\eta \mid \eta$是G到自身内的映照$\}$

(1)考究M关于乘法合成

因为对于η，$\rho \in M$，定义它们的积为$\eta\rho$，这是G到自身内两个映照连续施行的结果，仍然是G到自身内的一个映照，所以M关于乘法封闭，而且满足结合律。因此M关于乘法构成半群。

(2)考究M关于加法合成

1）∵$\eta + \rho$定义为$g(\eta + \rho) = (g\eta)(g\rho)$，$g\eta \in G$，$g\rho \in G$，∴$(g\eta)(g\rho) \in G$，∴$\eta + \rho$是G到自身内的映照，即$\eta + \rho \in M$，M关于加法封闭。

2）任取η，ρ，$\tau \in M$，对于任一$g \in G$

$\because g[\eta + (\rho + \tau)] = (g\eta)g(\rho + \tau) = g\eta \cdot (g\rho \cdot g\tau)$

$= (g\eta \cdot g\rho) \cdot g\tau = g(\eta + \rho)g\tau = g[(\eta + \rho) + \tau]$

$\therefore \eta + (\rho + \tau) = (\eta + \rho) + \tau$关于加法结合律成立。

3）设G的恒等元为e，对任意的$g\in G$，作映照η_0：

$$g\to e$$

显然$\eta_0\in M$，而且对任意$\eta\in M$

$$g(\eta_0+\eta)=(g\eta_0)\cdot(g\eta)=e\cdot(g\eta)=g\eta$$

$$g(\eta+\eta_0)=(g\eta)\cdot(g\eta_0)=(g\eta)\cdot e=g\eta$$

$$\therefore \eta_0+\eta=\eta+\eta_0=\eta$$

即η_0在M中起恒等元的作用。

4）对任意$\eta\in M$，定义ρ：$g\rho=(g\eta)^{-1}$，$(g\in G)$

显然，$\rho\in M$，而且

$$g(\eta+\rho)=g\eta\cdot g\rho=g\eta\cdot(g\eta)^{-1}=e$$

$$g(\rho+\eta)=g\rho\cdot g\eta=(g\eta)^{-1}g\eta=e$$

$$\therefore \eta+\rho=\rho+\eta=\eta_0$$

即ρ是η的负元。

故M关于加法构成群。特别当G是交换群，则因

$$g(\eta+\rho)=(g\eta)\cdot(g\rho)=(g\rho)(g\eta)=g(\rho+\eta)$$

$$\therefore \eta+\rho=\rho+\eta.$$

此时，M关于加法构成交换群。

（3）考究M中乘法对加法的分配律

$$\because g[\eta(\rho+\tau)]=(g\eta)(\rho+\tau)=(g\eta)\rho\cdot(g\eta)\tau$$

$$=g(\eta\rho)\cdot g(\eta\tau)=g(\eta\rho+\eta\tau)$$

$$\therefore \eta(\rho+\tau)=\eta\rho+\eta\tau$$

即左分配律成立。

但是，$g[(\rho+\tau)\eta]=[g(\rho+\tau)]\eta=(g\rho\cdot g\tau)\eta$

$$g\cdot(\rho\eta+\tau\eta)=g(\rho\eta)\cdot g(\tau\eta)$$

$\because \eta$不一定是同态映照，$\therefore$不一定有

$$(g\rho\cdot g\tau)\eta=g(\rho\eta)g(\tau\eta)$$

即不一定有$(\rho+\tau)\eta=\rho\eta+\tau\eta$

所以右分配律不一定成立。

(4)设η_1是G的恒等映照：$g\eta_1=g\ (g\in G)$

显然$\eta_1\in M$，而且，对任意的$\eta\in M$

$$g(\eta\eta_1)=(g\eta)\eta_1=g\eta,\quad\therefore\eta\eta_1=\eta$$

$$g(\eta_1\eta)=(g\eta_1)\eta=g\eta,\quad\therefore\eta_1\eta=\eta$$

因此η_1是M的乘法半群的恒等元。

第三章　环及域的扩张

习　题　37

1．如果A是一个环，对于它的所有元素a存在一个整数m，使$ma=0$，令S表二维组$(\bar{n},\ a)$的集合，这里$\bar{n}=n+(m)$是环$I/(m)$的元素，沿用课文中所述关于环B的相同的定义，但定义加法为

$$(\bar{n},\ a)+(\bar{q},\ b)=(\bar{n}+\bar{q},\ a+b)$$

定义乘法为

$$(\bar{n},\ a)\cdot(\bar{q},\ b)=(\bar{n}\bar{q},\ nb+qa+ab)$$

求验证：乘法是单值的，并且S是带恒等元素环，它是A的一个扩张，且对于所有的$c\in S$，$mc=0$．

〔证〕设A是环，令

$$S=\{(\bar{n},\ a)\mid\bar{n}\in I/(m),\ a\in A\}$$

(1)任取$(\bar{n},\ a)$，$(\bar{n}_1,\ a_1)$，$(\bar{q},\ b)$，$(\bar{q}_1,b_1)\in S$

若$(\bar{n},\ a)=(\bar{n}_1,\ a_1)$，$(\bar{q},\ b)=(\bar{q}_1,\ b_1)$，则

$a_1=a$，$n\equiv n_1(\mathrm{mod}\ m)$，$n_1=n+km$；$b_1=b$，

$q_1\equiv q\ (\mathrm{mod}\,m)$，$q_1=q+lm$．

$$\therefore (\bar{n}_1,a_1)(\bar{q}_1,b_1) = (\bar{n}_1\bar{q}_1,\ n_1b_1+q_1a_1+a_1b_1)$$
$$= (\overline{nq},(n+km)b+(q+lm)a+ab)$$
$$= (\overline{nq},\ nb+qa+ab+kmb+lma)$$
$$= (\overline{nq},\ nb+qa+ab) = (\bar{n},a)(\bar{q},b)$$

∴在S里所定义的乘法是单值的。

（2）1）由定义，S关于加法和乘法显然是封闭的。

2）关于加法满足结合律：

$$[(\bar{n},a)+(\bar{q},b)]+(\bar{p},c) = (\bar{n}+\bar{q}+\bar{p},a+b+c)$$
$$= (\bar{n},a)+[(\bar{q},b)+(\bar{p},c)]$$

3）关于加法满足交换律：

$$(\bar{n},a)+(\bar{q},b) = (\bar{n}+\bar{q},a+b) = (\bar{q}+\bar{n},b+a)$$
$$= (\bar{q},b)+(\bar{n},a)$$

4）$(\bar{o},o)\in S$是o元素：$(\bar{o},o)+(\bar{n},a) = (\bar{n},a)+(o,o)$
$$= (\bar{n},a)$$

5）$(\bar{n},a)$的负元素$(-\bar{n},\ -a)\in S$：

$$(\bar{n},a)+(-\bar{n},-a) = (o,o)$$

6）满足乘法的结合律：

$$[(\bar{n},a)(\bar{q},b)](\bar{p},c) = (\overline{nq},nb+qa+ab)(\bar{p},c)$$
$$= (\overline{nqp},nqc+npb+qpa+pab+nbc+pac+abc)$$
$$(\bar{n},a)[(\bar{q},b)(\bar{p},c)] = (\bar{n},a)(\overline{qp},qc+pb+bc)$$
$$= (\overline{nqp},nqc+npb+nbc+gpa+gac+pab+abc)$$
$$\therefore [(\bar{n},a)(\bar{q},b)](\bar{p},c) = (\bar{n},a)[(\bar{q},b)(\bar{p},c)]$$

7）满足乘法对加法的分配律：

$$(\bar{n},a)[(\bar{q},b)+(p,c)] = (\bar{n},a)(\bar{q}+\bar{p},b+c)$$
$$= (\overline{nq}+\overline{np},nb+nc+qa+pa+ab+ac)$$
$$= (\overline{nq},nb+qa+ab)+(\overline{np},nc+pa+ac)$$

$(\bar{n},a)(\bar{q},b)+(\bar{n},a)(\bar{p},c)$

同理可证$[(\bar{q},b)+(\bar{p},c)](\bar{n},a)=(\bar{q},b)(\bar{n},a)+(\bar{p},c)(\bar{n},a)$
因此S对于所定义的加法，乘法构成环（$\bar{1}$，0）是环S的恒等元：$(\bar{n},a)(\bar{1},0)=(\bar{1},0)(\bar{n},a)=(\bar{n},a)$

（3）令$A'=\{(\bar{0},a)|a\in A\}$ A'显然是S的子集。

∵当$a,b\in A$时，$a-b\in A$，$ab\in A$

∴$(\bar{0},a)-(\bar{0},b)=(\bar{0},a-b)\in A'$

$(\bar{0},a)(\bar{0},b)=(\bar{0},ab)\in A'$

∴A'是S的一个子环

作映照η：$a\rightarrow a'=(\bar{0},a)$，因为$(\bar{0},a)=(\bar{0},b)$必须且只须$a=b$，所以这个映照是1－1的，而且，对任意的$(\bar{0},c)\in A'$，A中都有原象$c$，所以$\eta$是A到$A'$上的1－1映照。

又∵$(a+b)^\eta=(\bar{0},a+b)=(\bar{0},a)+(\bar{0},b)=a^\eta+b^\eta$

$(ab)^\eta=(\bar{0},ab)=(\bar{0},a)(\bar{0},b)=a^\eta\cdot b^\eta$

∴η是A到A'上的同构映照，即$A\cong A'$，这也就是证明S是A的一个扩张。

（4）任取$C=(\bar{n},C)\in S$，

$mc=m(\bar{n},c)=(m\bar{n},mc)$

∵$m\bar{n}=m(n+(m))=mn+(m)=0+(m)$，即$m\bar{n}=\bar{0}$

$mc=0$

∴$mc=(\bar{0},0)$

2．如果A是一个整区，它含有元素a及$b\neq 0$，使对于某个整数m有$ab+mb=0$，求证：对于所有$C\in A$，

$$ca+mc=0=ac+mc$$

〔证〕∵$ab+mb=0$，两边左乘以c得

$$cab+cmb=cab+mcb=(ca+mc)b=0$$

$\because b \neq 0$，A是整区，$ca+mc \in A$,

$\therefore ca+mc=0$

若$c=0$，则显然有$ac+mc=0$

若$c \neq 0$，把等式$ca+mc=0$的两边右乘以c得：

$cac+mcc=cac+cmc=c(ac+mc)=0$

同样由于A是整区，$ac+mc=0$

3．如果A是一个整区，并令B 是课文中所作的环，验证：对于所有的$a \in A$，能使 $za=0$ 的B里的元素z 的全部Z是一个理想，并且B/Z是带恒等元素的一个整区。

〔证〕：设A是整区，令

$B=\{(n,\ a)|n \in I,\ a \in A\}$

在B中定义加法：$(n,a)+(m,b)=(n+m,a+b)$

在B中定义乘法：$(n,a)(m,b)=(nm,nb+ma+ab)$

则由书上所证知B，+，×构成环。

现考虑集合$Z=\{(n,z)|(n,z)(o,a)=(o,o)$，a 是A中任意元$\}$

任取$(n_1,\ z_1)$，$(n_2,\ z_2) \in Z$则

$[(n_1,z_1]-(n_2,z_2)](o,a)=(n_1z_1)(o,a)-(n_2,z_2)\cdot$

$(0,a)=0-0=0$

$\therefore (n_1,z_1)-(n_2,z_2) \in Z$

对任意的$(m,b) \in B$，$(n,z) \in Z$

$[(m,b)(n,z)](o,a)=(m,b)[(n,z)(o,a)]$

$=(m,b)\cdot(o,o)=(o,o)$

$[(n,z)(m,b)](o,a)=(n,z)[(m,b)(o,a)]$

$=(n,z)(o,ma+ba)$

$=(o,o)$，$(\because ma+ba \in A)$

$\therefore Z$是B的一个理想。

设$(n_1,a_1)+Z\neq 0+Z$,即$(n_1,a_1)\bar{\in} Z$,则存在$a\in A$,使得$(n_1,a_1)(0,a)=(0,n_1a+a_1a)\neq(0,0)$即$n_1a+a_1a\neq 0$,现假定有$(n_2,a_2)+Z\in B/Z$使得

$$[(n_2,a_2)+Z][(n_1,a_1)+Z]=(n_2,a_2)(n_1,a_1)+Z$$
$$=0+Z$$

要证$(n_2,a)+Z=0+Z$,即$(n_2,a_2)\in Z$

由$(n_2,a_2)(n_1,a_1)+Z=0+Z$知$(n_2,a_2)(n_1,a_1)\in Z$

即$(n_2,a_2)(n_1,a_1)(0,a)=(n_2a_2)(0,n_1a+a_1a)$

$$=(0,n_2(n_1a+a_1a)+a_2(n_1a+a_1a))=(0,0)$$

$\therefore A$中有元n_1a+a_1a使得

$$n_2(n_1a+a_1a)+a_2(n_1a+a_1a)=0$$

根据第2题得,对任意的$a\in A$,均有

$$n_2a+a_2a=0$$

$\therefore(n_2a_2)(0,a)=(0,n_2a+a_2a)=(0,0)$

即$(n_2,a_2)\in Z$,$\therefore(n_2,a_2)+Z$只能是B/Z的零元。

这就证得B/Z是整区,$\because(1,0)+Z\in B/Z$,且

$$[(n,a)+Z][(0,1)+Z]=[(1,0]+Z][(n,a)+Z]$$
$$=(n,a)(1,0)+Z=(n,a)+Z$$

$\therefore(1,0)+Z$是B/Z的恒等元素。

4.求证:$a\in A$时,形状如$a+Z$的陪集的集合$\overline{A}$是B/Z的一个子环,与A同构,故A被嵌入于B/Z内。

证: 令$\overline{A}=\{(0,a)+Z|a\in A\}$,显然$\overline{A}\subseteq B/Z$

任取$(0,a_1)+Z,(0,a_2)+Z\in\overline{A}$

$[(0,a_1)+Z]-[(0,a_2)+Z]=(0,a_1-a_2)+Z\in\overline{A}$

$[(0,a_1)+Z][(0,a_2)+Z]=(0,a_1a_2)+Z\in\overline{A}$

$\therefore$ $\overline{A}$是B/Z的一个子环。

作映照η：$a \longrightarrow (0,a)+Z$，显然$\eta$是A到$\overline{A}$上的映照，当$a=b$，则$(0,a)+Z=(0,b)+Z$，反之，若$(0,a)+Z=(0,b)+Z$则$(0,a)-(0,b)=(0,a-b)\in Z$，$\therefore$ 对任意的$c(\neq 0)\in A$，

$$(0,a-b)(0,c)=(0,(a-b)c)=(0,0)$$

即$(a-b)c=0$，$\because$ A是整区 $\therefore a-b=0$，即$a=b$

$\therefore \eta$是1－1的，又因

$$(a+b)\eta=(0,a+b)+Z=[(0,a)+Z]+[(0,b)+Z]=a\eta+b\eta$$

$$(ab)\eta=(0,ab)+Z=[(0,a)+Z][(0,b)+Z]=a\eta\cdot b\eta$$

$\therefore \eta$是A与$\overline{A}$一个同构，$\therefore A\cong\overline{A}$

即A被嵌入于B/Z内。

习　题　38

1．如果A是一个域，验证：$F=\overline{A}$。

〔证〕：$\because F=\{a/b|a,b\in A,\ b\neq 0\}$

$$\overline{A}=\{ab/b|a,b\in A,b\neq 0\}$$

显然有$\overline{A}\subset F$，任取$a/b\in F$，$a,b\in A$，$b\neq 0$

$\because$ A是域，$\therefore b^{-1}\in A$，$\therefore ab^{-1}\in A$，则

$a/b=a(b^{-1}b)/b=(ab^{-1})b/b=cb/b\in\overline{A}$ $\therefore F\subset\overline{A}$

因此得$F=\overline{A}$

2．求证：适合相消律的任一个交换半群可被嵌入于一群内。

〔证〕：设A是适合相消律的可换半群，则对任意的$a\in A$，

必有$a\neq 0$，因为如果$a=0$，则对任意的$b,c\in A,b\cdot 0=c\cdot 0=0$，由相消律成立得$b=c$，这是不可能的。令

$$B=\{(a,b)|a,b\in A\}$$

在B中定义关系～：当$ad=bc$时，$(a,b)\sim(c,d)$，关系～满足下列三个性质：

（1）$\because ab=ba\quad\therefore(a,b)\sim(a,b)$

（2）若$(a,b)\sim(c,d)$，则$ad=bc$，即$cb=da$

$\therefore(c,d)\sim(a,b)$

（3）若$(a,b)\sim(c,d)$，$(c,d)\sim(e,f)$则

$ad=bc,\quad cf=de$

把第一个等式两边同乘以f得

$adf=bcf=bde,$

$afd=bed$

$\because$在A中相消律成立，$\therefore af=be$，即$(a,b)\sim(e,f)$

$\therefore$关系～是等价关系，把B按等价关系～分类，得到等价类全体，记作$G=\{a/b,a,b\in A\}$，在G中定义乘法：

$a/b\cdot c/d=ac/bd$，并规定$a/b=c/d$，当且只当$ad=bc$

因为，如果$a/b=a'/b'$，$c/d=c'/d'$，则

$ab'=ba',\quad cd'=dc'$

$\therefore ab'cd'=ba'dc'$，即$acb'd'=bda'c'$

$\therefore ac/bd=a'c'/b'd'$　因此所定义的乘法单值

现证G关于所定义的乘法构成一个群。1）由乘法的定义，G显然是封闭的。

2）满足结合律：$[(a/b)(c/d)](e/f)=(a/b)[(c/d)(e/f)]=ace/bdf$

3）c/c是G的恒等元：$a/b\cdot c/c = c/c\cdot a/b = a/b$

4）对于$a/b\in G$，有$b/a\in G$，使得$a/b\cdot b/a = c/c$

∴G构成一个群

令$\bar{A} = \{ab/b,\ a,\ b\in A\}$，显然$\bar{A}\subset G$

∵$ab/b\cdot cd/d = abcd/bd = (ac)(bd)/bd = ef/f\in \bar{A}$

∴$\bar{A}$是群G的子半群

作映照η：$a\to ab/b$，显然η是A到$\bar{A}$上的映照。

若$a = c$，显然$ab/b = cd/d$，反之若$ab/b = cd/d$，则

$abd = cdb$，由相消律成立得$a = c$

∴η是1－1的。

又∵$(a\cdot c)\eta = acb/b = ab/b\cdot cb/b = a\eta\cdot c\eta$

∴η是A到$\bar{A}$上的一个同构，即$A\cong\bar{A}$，

因此证得A被嵌入群G中。

习　　题　　39

1．令B^*是序列$(a_0,\ a_1,\ a_2\cdots)$的全部，$a_i\in A$。关于等式，加法及乘法的定义与在B里的定义相同，求证B^*是一环，这个环叫做A上形式幂级数环，此后记作$A\langle X\rangle$。

〔证〕：令$B^* = \{(a_0,a_1,a_2,\cdots)|a_i\in$环$A\}$

定义：①$(a_0,a_2,a_2\cdots) = (b_0,b_1,b_2,\cdots)$，当且仅当

$a_i = b_i,\ i = 0,\ 1,\ 2,\ \cdots$

②$(a_0,a_1,a_2,\cdots) + (b_0,b_1,b_2,\cdots)$

$= (a_0+b_0,a_1+b_1,a_2+b_2\cdots)$

③$(a_0,a_1,a_2\cdots)(b_0,b_1,b_2\cdots) = (p_0,p_1,p_2\cdots)$

其中 $p_i = \sum\limits_{j+k=i} a_jb_k$

任取$(a_0,a_1,a_2,\cdots,),(b_0,b_1,b_2,\cdots),(c_0,c_1,c_2,\cdots)$
$\in B^*$

(1)显然$(a_0,a_1,a_2,\cdots)+(b_0,b_1,b_2,\cdots)\in B^*$，$(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2\cdots),\in B^*$ 所以B^*关于加法，乘法都封闭。

(2)$(a_0,a_1,a_2\cdots)+(b_0,b_1,b_2,\cdots)=(a_0+b_0,a_1+a_1,a_2+b_2\cdots)=(b_0+a_0,b_1+a_1,b_2+a_2,\cdots)=(b_0,b_1,b_2,\cdots)+(a_0,a_1,a_2,\cdots)$

(3)$(0,0,0,\cdots)$是B^*的零元：$(0,0,0,\cdots)+(a_0,a_1,a_2,\cdots)=(a_0,a_1,a_2,\cdots)+(0,0,0,\cdots)=(a_0,a_1,a_2,\cdots)$

(4)$(a_0,a_1,a_2,\cdots)$的负元是$(-a_0,-a_1,-a_2,\cdots)\in B^*$
$(a_0,a_1,a_2,\cdots)+(-a_0,-a_1,-a_2,\cdots)=(0,0,0,\cdots)$

(5)$[(a_0,a_1,a_2,\cdots)+(b_0,a_1,b_2,\cdots)]+(c_0,c_1,c_2,\cdots)$
$=(a_0,a_1,a_2,\cdots)+[(b_0,b_1,b_2,\cdots)+(c_0,c_1,c_2,\cdots)]$
$=(a_0+b_0+c_0,a_1+b_1+c_1,a_2+a_2+c_2,\cdots)$ ∴关于加法满足结合律。

(6)$[(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2,\cdots)](c_0,c_1,c_2,\cdots)$里下标为i的项是$\sum\limits_{m+l=i}(\sum\limits_{j+k=m}a_j b_k)c_l=\sum\limits_{j+k+l=i}a_j b_k c_l$

同理，$(a_0,a_1,a_2,\cdots)[(b_0,b_1,b_2,\cdots)(c_0,c_1,c_2,\cdots)]$里下标为i的项是

$$\sum_{m+j=i}a_j(\sum_{k+l=m}b_k c_l)=\sum_{j+k+l=m}a_j b_k c_l$$

∴$[(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2,\cdots)](c_0,c_1,c_2,\cdots)$
$=(a_0,a_1,a_2\cdots)[(b_0,b_1,b_2,\cdots)(c_0,c_1,c_2,\cdots)]$关于乘法结合律成立

(7) $(a_0,a_1,a_2,\cdots)[(b_0,b_1,b_2,\cdots)+(c_0,c_1,c_2,\cdots)]$
里下标为 i 的项是

$$\sum_{j+k=i} a_j(b_k+c_k)=\sum_{j+k=i} a_jb_k+\sum_{j+k=i} a_jc_k$$

上式右边也就是$(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2,\cdots)+(a_0,a_1,a_2,\cdots)(c_0,c_1,c_2,\cdots)$中下标为i的项

$\therefore (a_0,a_1,a_2,\cdots)[(b_0,b_1,b_2,\cdots)+(c_0,c_1,c_2,\cdots)]$
$(a_0,a_1,a_2,\cdots)(b_0,b_1,b_2,\cdots)+(a_0,a_1,a_2,\cdots)(c_0,c_1,c_2,\cdots)$

同理可证：$[(b_0,b_1,b_2,\cdots)+(c_0,c_1,c_2,\cdots)](a_0,a_1,a_2,\cdots)=(b_0,b_1,b_2,\cdots)(a_0,a_1,a_2,\cdots)+(c_0,c_1,c_2,\cdots)(a_0,a_1,a_2,\cdots)$

∴乘法对加法的分配律成立。

因此，B^*构成环。

2. 令S是任一个半群，并令A是任一个环，令a (s) 是定义在s上的函数，它的值$\in A$,且除有限个s外，$a(s)=0$，令B是这样函数a(s)的集合，在B里加法及乘法定义为

$$(a+b)(s)=a(s)+b(s)$$
$$(ab)(s)=\sum_{tu=s} a(t)b(u)$$

验证：B是一个环，叫做**半群环**。

〔证〕：(1)因A是一个环，若$a(s),b(s)\in A$，则$a(s)+b(s)\in A$.

同样 $\sum_{tu=s} a(t)b(u)\in A$，且显然除有限个s外，$a(s)+b(s)=0$，$(ab)(s)=\sum a(t)b(u)=0 \qquad (tu=s)$

(2) $\because (a+b)(s)=a(s)+b(s)=b(s)+a(s)=(b+a)(s)$

$\therefore$ 在B里满足交换律

(3) 对所有的 $s\in S$，定义函数 $0(s)\equiv 0$，$\because 0\in A$，$\therefore 0(s)\in B$，$0(s)$是B的零元：$(a+0)(s)=a(s)+0(s)$ $=a(s)=(0+a)(s)$

(4) $a(s)$的负元 $(-a)(s)=-a(s)$，显然除有限个s外 $(-a)(s)=0$，$\therefore (-a)(s)\in B$

(5) $[(ab)\cdot c](s)$

$$=\sum_{tu=s} ab(t)c(u)=\sum_{tu=s}\left(\sum_{xy=t} a(x)b(y)\right)c(u)$$

$$=\sum_{xyu=s}\left(a(x)b(y)\right)(cu)=\sum_{xyu=s} a(x)\left(b(y)c(u)\right)$$

$$=\sum_{xt=s}a(x)\left(\sum_{yu=t}b(y)c(u)\right)=\sum_{xt=s} a(x)(bc)(t)=(a\cdot(bc))(s)$$

$\therefore$ 关于乘法结合律成立

(6) $[a(b+c)](s)=\sum\limits_{tu=s} a(t)\cdot(b+c)(u)=\sum\limits_{tu=s} a(t)$ $(b(u)+c(u))=\sum\limits_{tu=s}a(t)b(u)+\sum\limits_{tu=s}a(t)c(u)=ab(s)+ac(s)$

$=(ab+ac)(s)$

同理可证$(b+c)a(s)=(ba+ca)(s)$

$\therefore$ 乘法对加法的分配律成立。

因此B是一个环。

3．验证：由非负整数与加结合成组织的半群所决定的半群环，是上面所作的环$A[x]$。

〔证〕：设I_+表示集合为非负整数，合成为加法的半群

令$B=\{a(s)\mid s\in I_+, a(s)\in$环$A$,除有限个$s$外,$a(s)=0\}$

由上题知B关于加法与乘法:

$$(a+b)(s)=a(s)+b(s)$$

$$ab(s)=\sum_{t+u=s} a(t)b(u)$$

构成由I_+所决定的半群环。

任取$a(s)\in B$，设$a(0)=a_0$，$a(1)=a_1$，$a(2)=a_2$，… $a(n)=a_n$，$a(n+1)=0$，$a(n+2)=0$，…，

作映照η：$a(s)\to a_0+a_1x+a_2x^2+\cdots+a_nx^n$（$x$为超越元）

$$b(s)\to b_0+b_1x+b_2x^2+\cdots+b_mx^m$$

当$a(s)=b(s)$时,显然$n=m$,且$a_i=a(i)=b(i)=b_i$

$$\therefore a_0+a_1x+a_2x^2+\cdots+a_nx^n=b_0+b_1x+b_2x^2+\cdots+b_nx^n$$

反之,若$a(s)\neq b(s)$,则$a_0,a_1,a_2,\cdots,a_n$与b_0，b_1，…，b_m不全对应相同$\therefore a_0+a_1x+a_2x^2+\cdots+a_nx^n\neq b_0+b_1x+b_2x^2+\cdots+b_mx^m$ 而且对任意的$a_0+a_1x+a_2x^2+\cdots+a_nx^n\in A[x]$，可构造函数$a(s)$，使得$a(0)=a_0$,$a(1)=a_1$,$a(2)=a_2$,…。$a(n)=a_n$。实际上，函数

$$a(s)=\begin{cases}(a_1-a_0)s+a_0, & \text{当 } 0\leqslant s<1\\ (a_2-a_1)(s-1)+a_1, & \text{当 } 1\leqslant s<2\\ \cdots\cdots & \\ (a_n-a_{n-1})(s-n+1)+a_{n-1}, & \text{当 } n-1\leqslant s\leqslant n\end{cases}$$

$a(s)=0$（$s>n$）就是所求的。

由此可见η是B到$A(x)$上的1－1映照。

设$a(s)$只有对n个s不为0，$b(s)$只有对m个s不为0，其他全为0，若$n>m$，由$(a+b)(s)=a(s)+b(s)$可知$(a+b)(s)$最多对n个s不为0。

$\therefore [(a+b)(s)]\eta = (a+b)(0)+(a+b)(1)x+(a+b)(2)x^2+\cdots+(a+b)(n)x^n = a(0)+a(1)x+a(2)x^2+\cdots+a(n)x^n+b(0)+b(1)x+b(2)x^2+\cdots+b(n)x^n = a_0+a_1x+a_2x^2+\cdots+a_nx^n+b_0+b_1x+b_2x^2+\cdots+b_mx^m+\cdots+0x^n = a(s)\eta+b(s)\eta$

又由 $ab(s)=\sum\limits_{t+u=s} a(t)b(u)$ 可知 $ab(s)$ 最多对 $m+n$ 个 s 不为 0。

$\therefore [ab(s)]\eta = ab(0)+ab(1)x+ab(2)x^2+\cdots ab(i)x^i+\cdots+ab(n+m)x^{m+n} = a(0)b(0)+[a(0)b(1)+a(1)b(0)]x+\cdots+(\sum\limits_{j+k=i} a(j)b(k))x^i+\cdots+a(n)b(m)x^{m+n} = [a(0)+a(1)x+\cdots+a(n)x^n][b(0)+b(1)x+\cdots+b(m)x^m] = a(s)\eta\cdot b(s)\eta$

因此 η 是B到A[x]上的一个同构，即 $B\cong A[x]$

习　题　40

1. 如果 $f(x)=a_0+a_1x+\cdots+a_nx^n$，定义 $f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}$

求证：通常的法则

$$(f+g)'=f'+g' \quad (cf)'=cf' \quad c\in A$$

$$(fg)'=fg'+f'g$$

证：不妨设 $f(x)=a_0+a_1x+\cdots+a_nx^n$，$g(x)=b_0+b_1x+\cdots b_nx^n$

(1) $\because f(x)+g(x)=\sum\limits_{i=0}^{n}(a_i+b_i)x^i$

$$\therefore [f(x)+g(x)]' = \sum_{i=1}^{n} i(a_i+b_i)x^{i-1}$$

$$= \sum_{i=1}^{n} ia_i x^{i-1} + \sum_{i=1}^{n} ib_i x^{i-1} = f'(x)+g'(x)$$

$$(2) \because cf(x) = c\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (ca_i) x^i$$

$$\therefore [cf(x)]' = \sum_{i=1}^{n} i(ca_i) x^{i-1} = \sum_{i=1}^{n} c(ia_i) x^{i-1}$$

$$= c\sum_{i=1}^{n} (ia_i) x^{i-1} = cf'(x)$$

$$(3) \because f(x)g(x) = \sum_{k=0}^{2n} \sum_{i+j=k} a_i b_j x^k$$

$$\therefore (f(x)\cdot g(x))' = \sum_{k=1}^{2n} \sum_{i+j=k} ka_i b_j x^{k-1} = \sum_{k=1}^{2n} \sum_{i+j=k}$$

$$(i+j)a_i b_j x^{k-1} = \sum_{k=1}^{2n} \sum_{i+j=k} (ia_i)b_j x^{k-1} + \sum_{k=1}^{2n} \sum_{i+j=k} a_i(jb_j)$$

$$x^{k-1} = \left(\sum_{k=1}^{n} ka_k x^{k-1}\right)\left(\sum_{k=0}^{n} b_k x^k\right) + \left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{k=1}^{n}\right.$$

$$\left. kb_k x^{k-1}\right) = f'(x)g(x) + f(x)g'(x)$$

2．求证：李卡尼兹（Leibniz）定理

$$(fg)^{k} = \sum_{0}^{k} c_k^i f^{(i)} g^{(k-i)}$$

这里$f^{(i)}=(f^{(i-1)})'$，$f^{(0)}=f$。

〔证〕：对k施行数学归纳法

当$k=1$时，此即上题中所证的结论，定理成立。

设$k=n$时，定理成立，即$(fg)^{(n)}=\sum_{i=0}^{n}C_n^i f^{(i)}g^{(n-i)}$，则

$$(fg)^{(n+1)}=((fg)^{(n)})'=\sum_{i=0}^{n}c_n^i(f^{(i)}g^{(n-i)})'=$$

$$\sum_{i=0}^{n}c_n^i(f^{(i)\prime}g^{(n-1)}+f^{(i)}g^{(n-1)\prime})$$

$$=\sum_{i=0}^{n}c_n^i f^{(i+1)}g^{(n-1)}+\sum_{i=0}^{n}c_n^i f^{(i)}g^{(n-i+1)}$$

$$=\sum_{i=1}^{n+1}c_n^{i-1}f^{(i)}g^{(n-i+1)}+\sum_{i=0}^{n}c_n^i f^{(i)}g^{(n-i+1)}$$

$$=c_n^0 fg^{(n+1)}+\sum_{i=1}^{n}c_n^{i-1}f^{(i)}g^{(n-i+1)}\sum c_n^i f^{(i)}g^{(n-i+1)}$$

$$+c_n^n f^{(n+1)}g$$

$$=c_{n+1}^0 fg^{(n+1)}+\sum(c_n^{i-1}+c_n^i)f^{(i)}g^{(n-i+1)}+$$

$$c_{n+1}^{n+1}f^{(n+1)}g$$

$$=\sum_{i=0}^{n+1}c_{n+1}^i f^{(i)}(g^{n+1-i})$$

由此可知，对任意自然数k，定理成立。

习　　题　　41

1．令$S=R_0[x]/(x^3+3x-2)$，求把S的元素

(a)　　$(2\bar{x}^2+\bar{x}-3)(3\bar{x}^2-4\bar{x}+1)$

(b)　　$(2\bar{x}^2+4\bar{x}-5)^{-1}$

列成$\bar{x}$的多项式，其次数<3，（R_0是有理数域）

〔解〕：(a) $(2\bar{x}^2+\bar{x}-3)(3\bar{x}^2-4\bar{x}+1)$

$$=6\bar{x}^4-5\bar{x}^3-11\bar{x}^2+13\bar{x}-3\triangleq g(\bar{x})$$

$$f(\bar{x})=\bar{x}^3+3\bar{x}-2$$

运用带余除法，以$f(\bar{x})$除$g(\bar{x})$得

$$(2\bar{x}^2+\bar{x}-3)(3\bar{x}^2-4\bar{x}+1)=(\bar{x}^3+3\bar{x}-2)(6\bar{x}-5)+(-29\bar{x}^2+40\bar{x}-13)$$

$$=-29\bar{x}^2+40\bar{x}-13\quad(\because \bar{x}^3+3\bar{x}-2=0)$$

(b)：令$f(x)=x^3+3x-2, g(x)=2x^2+4x-5$

对$f(x), g(x)$作辗转相除法得：

$$f(x)=(\frac{1}{2}x-1)g(x)+(\frac{19}{2}x-7)\cdots\cdots(1)$$

$$g(x)=(\frac{4}{19}x+\frac{208}{19^2})(\frac{19}{2}x-7)-\frac{349}{19^2}\cdots\cdots\cdots(2)$$

由(1)式得 $0=\overline{f(x)}=f(\bar{x})=(\frac{1}{2}\bar{x}-1)g(\bar{x})+(\frac{19}{2}\bar{x}-7)$

即$\frac{19}{2}\bar{x}-7=-(\frac{1}{2}\bar{x}-1)g(\bar{x})\cdots\cdots(3)$

由(2)式得$g(\bar{x})=(\frac{4}{19}\bar{x}+\frac{208}{19^2})(\frac{19}{2}\bar{x}-7)-\frac{349}{19^2}$

即 $-\frac{19^2}{349}[g(\overline{x})-(\frac{4}{19}\overline{x}+\frac{208}{19^2})(\frac{19}{2}\overline{x}-7)]=1\cdots\cdots(4)$

把(3)式代入(4)式得

$$-\frac{19^2}{349}[g(\overline{x})+(\frac{4}{19}\overline{x}+\frac{208}{19^2})(\frac{1}{2}\overline{x}-1)g(\overline{x})]=1$$

即 $-\frac{19^2}{349}[1+(\frac{4}{19}\overline{x}+\frac{208}{19^2})(\frac{1}{2}\overline{x}-1)]g(\overline{x})=1$

$$\therefore\ g(\overline{x})^{-1}=-\frac{19^2}{349}[1+(\frac{4}{19}\overline{x}+\frac{208}{19^2})(\frac{1}{2}\overline{x}-1)]$$

$$=-\frac{19^2}{349}+(\frac{-4\times19}{349}\overline{x}-\frac{208}{349})(\frac{1}{2}\overline{x}-1)$$

$$=\frac{-38}{349}\overline{x}^2-\frac{28}{349}\overline{x}-\frac{153}{349}$$

即 $(2\overline{x}^2+4\overline{x}-5)^{-1}=-\frac{38}{349}\overline{x}^2-\frac{28}{349}\overline{x}-\frac{153}{349}$

2. 如果 $g(x)$ 有一个平方因子 $(f(x)=[f_1(x)]^2f_2(x), \deg f_1(x)>0)$

验证：$S=F[x]/(f(x))$ 含有非零无势元素

证：令 $g(x)=f_1(x)f_2(x)$

$$\overline{g(x)}=g(x)+(f(x))\in F[x]/(f(x))$$

$$\overline{g(x)}^2=\overline{f_1(x)f_2(x)}^2=\overline{f_1^2(x)f_2(x)\cdot f_2(x)}$$

$$=\overline{f(x)\cdot f_2(x)}=\overline{f(x)}\cdot\overline{f_2(x)}=0\cdot\overline{f_2(x)}=0$$

$\therefore\overline{g(x)}$ 是 $F[x]/(f(x))$ 的幂零元（即无势元）

又 $\because \deg f(x)=\deg f_1(x)+\deg f_1(x)+\deg f_2(x)$

$$>\deg f_1(x)+\deg f_2(x)=\deg g(x)$$

即 $\deg f(x)>\deg g(x)$ $\therefore f(x)\nmid g(x)$ 即 $g(x)\notin(f(x))$ 因此 $g(x)$ 不是 $F[x]/(f(x))$ 的零元，

即 $\overline{g(x)}$ 是 $F[x]/(f(x))$ 非零无势元。

习　题　42

1. 设$a_n \not\equiv 0 \pmod p$，则同余式$a_0+a_1x+\cdots\cdots+a_nx^n\equiv 0 \pmod p$在I里至多只有 n 个非同余解。

〔证〕∵若x是同余式$a_0+a_1x+\cdots+a_nx^n\equiv 0 \pmod p$的解，

则$\overline{a_0+a_1x+\cdots+a_nx^n}=\bar a_0+\bar a_1\bar x+\cdots\bar a_n\bar x^n=\bar o$

即$\bar x$是方程式$\bar a_0+\bar a_1\bar x+\cdots+\bar a_n\bar x^n=\bar o$的解

反之，若$\bar x$是方程式$\bar a_0+\bar a_1\bar x+\cdots+\bar a_n\bar x^n=\bar o$的解，则

$$\overline{a_0+a_1x+\cdots+a_nx^n}=\bar o$$

即$a_0+a_1x+\cdots+a_nx^n\equiv 0 \pmod p$

∴ x 是同余式$a_0+a_1x+\cdots+a_nx^n\equiv 0 \pmod p$的解

因此解同余式$a_0+a_1x+\cdots+a_nx^n\equiv 0 \pmod p$等价于解方程式$\bar a_0+\bar a_1\bar x+\cdots+\bar a_n\bar x^n=\bar o$

∵$a_n\not\equiv 0 \pmod p$　∴ $\bar a_n\neq\bar o$

I/(p)（p是质数）是域，$\bar a_i(i=0,1,\cdots,n)\in I/(p)$

∴ $\bar a_0+\bar a_1\bar x+\cdots+\bar a_n\bar x^n$是系数在域 I/(p)中次数为n的多项式，根据定理 7，它在I/(p)中最多只有 n 个不同的根，设$\bar x_i$，$\bar x_j$是其中任两个根，$\bar x_i\neq\bar x_j$

则$\bar x_i-\bar x_j=\overline{x_i-x_j}\neq 0$，∴ $x_i-x_j\not\equiv 0 \pmod p$

即$x_i\not\equiv x_j \pmod p$，从而证得同余式$a_0+a_1x+\cdots+a_nx^n\equiv 0 \pmod p$在I里至多只有 n 个非同余解。

2. 如果F是含有q个元素a_i的一个有限域，求证：在F〔x〕里

$$h(x)=x^q-x=(x-a_1)(x-a_2)\cdots(x-a_q)$$

〔证〕：∵F是有限域，其元数为q，∴F非零元所成的乘群元数为q－1，根据Lagrange定理，对F的任一非零元a_i都有

$a_i^{q-1}=1$　即$a_i^q=a_i$

∴F所含的q个元$a_1,a_2,\cdots,a_q$都是多项式

$$h(x)=x^q-x \text{ 的根}$$

而h(x)是q次多项式，它在F中最多只有q个根，所以

$a_1,a_2,\cdots a_q$是h(x)全部的根

即$h(x)=(x-a_1)(x-a_2)\cdots(x-a_q)$

3．如果p是素数，求证：$(p-1)!\equiv-1 \pmod p$ 这叫做威尔孙（Wilson）定理。

〔证〕：∵I/(p)是含有p个元($\overline{0},\overline{1}\cdots,\overline{P-1}$)的有限域，由第2题，$x^p-x=(x-\overline{0})(x-\overline{1})\cdots(x-\overline{P-1})$

$=x(x-\overline{1})\cdots(x-\overline{P-1})$

∴$x^{p-1}-1=(x-\overline{1})\cdots(x-\overline{P-1})$

令$x=\overline{P}=\overline{0}$ 代入，当$P\neq2$时即得$\overline{(p-1)!}=-1$当$p=2$时，显然$(2-1)!\equiv-1 \pmod 2$

∴$(p-1)!\equiv-1 \pmod p$

4．验证：多项式x^3-x在I/(6)里有6个根。

〔证〕：$I/(6)=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$

当$x_1=\overline{0}$时，$x_1^3-x_1=\overline{0}-\overline{0}=\overline{0}$

当$x_2=\overline{1}$时，$x_2^3-x_2=\overline{1}^3-\overline{1}=\overline{1}-\overline{1}=\overline{0}$

当$x_3=\overline{2}$时，$x_3^3-x_3=\overline{2}^3-\overline{2}=\overline{8}-\overline{2}=\overline{2}-\overline{2}=\overline{0}$

当$x_4=\overline{3}$时，$x_4^3-x_4=\overline{3}^3-\overline{3}=\overline{27}-\overline{3}=\overline{3}-\overline{3}=\overline{0}$

当$x_5=\overline{4}$时，$x_5^3-x_5=\overline{4}^3-\overline{4}=\overline{64}-\overline{4}=\overline{4}-\overline{4}=\overline{0}$

当$x_6=\overline{5}$时，$x_6^3-x_6=\overline{5}^3-\overline{5}=\overline{125}-\overline{5}=\overline{5}-\overline{5}=\overline{0}$

∴I/(6)的6个元都是x^3-x的根

5．验证：多项式x^2+1在实四维数环Q里有无限个

根。

〔证〕：设$\alpha=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$，（$\alpha_0,\alpha_1,\alpha_2,\alpha_3$是实数）$\in Q$

$\because \alpha^2=(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)^2=\alpha_0^2-\alpha_1^2-\alpha_2^2-\alpha_3^2+2\alpha_0\alpha_1 i+2\alpha_0\alpha_2 j+2\alpha_0\alpha_3 k$

$\therefore$只要取$\alpha\in Q$满足$\alpha_0=0$且$\alpha_1^2+\alpha_2^2+\alpha_3^2=1$，则这样的$\alpha$就是多项式$x^2+1$的根，而满足关系式

$$\alpha_1^2+\alpha_2^2+\alpha_3^2=1$$

的α有无限多个，$\therefore$多项式x^2+1在Q中有无限多个根

习　　题　　43

1．设x_i是代数无关元素，验证：一个环$A[x_1,x_2,\cdots,x_r]$还可由负非整数i_j的r维组$(i_1,j_2,\cdots i_r)$的半群S的A上半群环得出，这里合成是

（＊）$(i_1,i_2,\cdots i_r)(j_1,j_2\cdots,j_r)=(i_1+j_1,i_2+j_2,\cdots i_r+j_r)$

〔证〕：令$S=\{(i_1,i_2,\cdots,i_r)|i_j,j=1,2,\cdots,r$是非负整数$\}$是关于合成（＊）的半群，$B=\{a(s)|s\in S,\ a(s)\in A$，$a(s)$只对有限个s不为0$\}$是由s决定的A上的半群环．

设$a(i_1,i_2,\cdots,i_r)=a_{i_1 i_2\cdots i_r}$

作B到$A[x_1,x_2,\cdots,x_r]$内的映照η：

$$a(i_1 i_2,\cdots i_r)\to\sum a_{i_1 i_2\cdots i_r}x_1^{i_1}x_2^{i_2}\cdots x_r^{i_r}$$

$\because x_1,x_2\cdots,x_r$是A上代数无关元

$\therefore$如果$\sum a_{i_1 i_2\cdots i_r}x_1^{i_1}x_2^{i_2}\cdots x_r^{i_r}=\sum b_{i_1 i_2\cdots i_r}\cdot x_1^{i_1}x_2^{i_2}\cdots x_r^{i_r}$

则$a_{i_1 i_2\cdots i_r}=b_{i_1 i_2\cdots i_r}$，$\therefore a(i_1,i_2,\cdots i_r)=b(i_1 i_2,\cdots i_r)$

$\therefore \eta$ 是 1－1 的。而且，对于任意的 $\sum C_{i_1 i_2 \cdots i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}$，由于其项数有限，$\therefore$ 可造函数 $C(i_1 i_2 \cdots i_r)$ 使得

$$C(i_1, i_2, \cdots i_r) = C_{i_1 i_2, \cdots i_r}$$

$\therefore \eta$ 是到上的。

又 $\because [(a+b)(i_1, i_2, \cdots, i_r)]\eta = [a(i_1, i_2, \cdots i_r) + b(i_1, i_2, \cdots, i_r)]\eta$

$$= \sum (a_{i_1 i_2 \cdots i_r} + b_{i_1 i_2 \cdots i_r}) x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}$$

$$= \sum a_{i_1 i_2, \cdots i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} + \sum b_{i_1 i_2 \cdots i_r} x_1^{i_1} \cdot x^{i_2} \cdots x_r^{i_r}$$

$$= a(i_1, i_2 \cdots i_r)\eta + a(i_1 i_2, i_r)\eta$$

$$(ab)(i_1 i_2, \cdots, i_r)\eta = [\sum a(j_1, j_2, \cdots, j_r) b(k_1, k_2 \cdots, k_r)]\eta$$

$$(j_1 \cdots j_r) \cdot (k_1, \cdots k_r) = (j_1, j_2, \cdots j_r)$$

$$= \sum (\sum a_{i_1 i_2 \cdots i_r} b_{k_1 k_2 \cdots k_r}) x_1^{i^1} x_2^{i^2} \cdots x_r^{ir}$$

$$(i_1 \cdots i_r)(k_1 \cdots k_r) = (i_1 i_2, \cdots i_r)$$

$$= (\sum a_{i_1 i_2 \cdots i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r})(\sum b_{i_1 i_2 \cdots i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r})$$

$$= (a(i_1, i_2, \cdots i_r)\eta) \cdot (b(i_1, i_2, \cdots i_r)\eta)$$

$\therefore \eta$ 是B到 $A[x_1, x_2, \cdots x_r]$ 上的同构，即 $B \cong A[x_1, x_2, \cdots, x_r]$

习　题　44

1．求以初等对称函数表示 $\sum\limits_{i,j,k\neq} x_i^2 x_j^2 x_k \ (n \geq 5)$

〔解〕：由指数型为22100；21110：11111。知

$$\sum_{i,j,k\neq} x_i^2 x_j^2 x_k = p_2p_3 + ap_1p_4 + bp_5$$

然后确定系数a，b；分别令 $x_1=\cdots=x_4=1$，$x_5=\cdots=x_n=0$；及 $x_1=\cdots=x_5=1$，$x_6=\cdots=x_n=0$，得a＝－3；b＝5则

$$\sum_{i,j,k\neq} x_i^2 x_j^2 x_k = p_2p_3 - 3p_1p_4 + 5p_5$$

2．令$\Delta=\prod_{i<j}(x_i-x_j)$．如果$\eta$是一个对换，验证$\eta^*=-\Delta$。使用这个结果证明：如果$\tau$是一个置换它有一个分解是偶（奇）数个对换的积，则$\tau$的任一个因子分解成对换的积必含着偶（奇）数个对换。

〔证〕：设对换$\eta=(x_k x_l)$是相邻两文字的对换，即$x_l=x_{k+1}$。把Δ写成：$\Delta=(x_k-x_l)\prod_{i\neq k,l}(x_i-x_k)(x_i-x_l)\delta$．其中$\delta$不包含$x_k$及$x_l$。则在$\Delta$上施行对换$(x_kx_l)$后，$(x_i-x_k)(x_i-x_l)$及$\delta$都不变动，但$(x_k-x_l)$变了符号，即$\Delta\eta^*=-\Delta$。其次任意对换可表成奇数个相邻两文字对换的乘积，故对任意对换η也有$\Delta\eta^*=-\Delta$。

于是对Δ连续施行偶数个对换，结果仍是Δ，若连续施行奇数个对换，则结果是$-\Delta$。而在Δ上施行一个置换τ后的结果是一定的。因此若一置换τ它有一个分解是偶（奇）数个对换的积，则τ的任一个因子分解成对换的积必含偶(奇)数个对换。否则符号会改变。

3．验证：$\triangle^2$是对称的。就 $r=3$ 把$\triangle^2$用初等对称函数表出。

〔证〕：依上题，若置换τ是奇置换，则$\triangle\tau^*=-\triangle$。于是 $\triangle^2\tau^*=(-\triangle)^2=\triangle^2$。若$\tau$是偶置换，则$\triangle\tau^*=\triangle$。有$\triangle^2\tau^*=\triangle^2$。因此对任意置换$\tau$，$\triangle^2$都保持不变，故$\triangle^2$是对称的。

当$r=3$时，$\triangle^2=(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$
$=x_1^4x_2^2+\cdots$由指数型为420，411，330，321，222。知

$$\triangle^2=p_1^2p_2^2+ap_1^3p_3+bp_2^3+cp_1p_2p_3+dp_3^2$$

利用待定系数法，分别令$x_1=x_2=1$，$x_3=0$；$x_1=2$，$x_2=x_3=-1$；$x_1=-1$，$x_2=x_3=2$及$x_1=x_2=x_3=1$，代入原方程，依次得$b=-4$，$d=-27$，$a=-4$，$c=18$　故

$$\triangle^2=p_1^2p_2^2-4p_1^3p_3-4p_2^3+18p_1p_2p_3-27p_3^2$$

4．验证：对称多项式$S_k=\sum x^k$适合牛顿（Newton）恒等式。

$$S_k-p_1S_{k-1}+p_2S_{k-2}-\cdots+(-1)^{k-1}p_{k-1}S_1+(-1)^k kp_k=0\quad(k=1,\ 2,\ \cdots,\ n)$$

〔证〕：由$k\leqslant n$，我们有

$$S_{k-i}p_i=\sum x_1^{k-i}\sum x_1x_2\cdots x_i$$
$$=\sum x_1^{k-i+1}x_2\cdots x_i+\sum x_1^{k-i}x_2\cdots x_{i+1}$$

上式对$k-i>1$时是成立的，当$k-i=1$时，即$i=k-1$时有

$$S_1p_{k-1}=\sum x_1\sum x_1x_2\cdots x_{k-1}$$
$$=\sum x_1^2x_2\cdots x_{k-1}+k\sum x_1x_2\cdots x_k$$
$$=\sum x_1^2x_2\cdots x_{k-1}+kp_k$$

因之，$S_{k-1}p_1=\sum x_1^k+\sum x_1^{k-1}x_2=S_k+\sum x_1^{k-1}x_2$，

$$S_{k-2}p_2=\sum x_1^{k-1}x_2+\sum x_1^{k-2}x_2x_3,$$

$\cdots$

$$S_{k-i}p_i=\sum x_1^{k-i+1}x_2\cdots x_i+\sum x_1^{k-i}x_2\cdots x_{i+1}$$

$$S_{k-i-1}p_{i+1}=\sum x_1^{k-i}x_2\cdots x_{i+1}+\sum x_1^{k-i-1}x_2\cdots x_{i+2},$$

$\cdots$

$$S_1p_{k-1}=\sum x_1^2x_2\cdots x_{k-1}+kp_k.$$

交错乘以－1及＋1再相加，则右边的Σ两两相消而只剩下$-S_k+(-1)^{k-1}kp_k$，将这两项移到左边即得所求公式

$$S_k-p_1S_{k-1}+p_2S_{k-2}-\cdots+(-1)^{k-1}p_{k-1}S_1+(-1)^k kp_k=0\quad(k=1,2,\cdots,n)$$

习　题　45

1．求证定理10的拓广定理：如果$f(x_1,\cdots,x_r)$是多项式，其系数属于一个无限域F，如果能使另一个非零多一个项式$g(x_1,\cdots,x_r)$的值$g(c_1,c_2,\cdots c_r)\neq 0$的所有$(c_1,c_2,\cdots,c_r)$都使$f(c_1,c_2,\cdots,c_r)=0$，则$f(x_1,x_2,\cdots x_r)=0$

〔证〕：设$g(x_1,\cdots,x_r)(\neq 0)$，$f(x_1,\cdots x_r)\in F[x_1,\cdots,x_r]$。$f\cdot g(x_1,\cdots x_r)=f(x_1,\cdots x_r)g(x_1,\cdots,x_r)$

假设$f(x_1,\cdots,x_r)\neq 0$，则$fg(x_1,\cdots,x_r)$是$F[x_1,\cdots,x_r]$中非零多项式，根据定理10，在F中存在$c_1,\cdots,c_r$使$fg(c_1,\cdots,c_r)\neq 0$，即$f(c_1,\cdots c_r)g(c_1,\cdots,c_r)\neq 0$但这与已知矛盾，因为任一组$(c_1,\cdots c_r)$或者使$g(c_1,\cdots,c_r)=0$或者使$g(c_1,\cdots c_r)\neq 0$，而$f(c_1,\cdots,c_r)=0$

$\therefore f(c_1\cdots c_r)g(c_1,\cdots c_r)=0$。

因而得$f(x_1, x_1, \cdots x_r)=0$

2．令F是含有q个元素的一个有限域，求证：

如果$f(x_1\cdots x_r)$是一个非零多项式，对于每个x_i的次数都$<q$，则F里存在C_i，使$f(c_1,c_1,\cdots,c_r)\neq 0$。

〔证〕：对r施行归纳法。

当$r=1$时，设$\deg f(x_1)=m$。则由定理7知，$f(x_1)$在F中至多有m个零点，但因$m<$F的元数q。

∴F中必有一元c_1，使得$f(c_1)\neq 0$，所以对$r=1$命题成立。

设当$r=k$时命题成立。考虑$r=k+1$的情形。

把$f(x_1,x_2,\cdots,x_k,x_{k+1})$改写为

$$f(x_1,,\cdots,x_k,x_{k+1})=B_0(x_1,\cdots,x_k)+B_1(x_1,\cdots x_k)x_{k+1}+\cdots+B_n(x_1,\cdots,x_k)x_{k+1}^n$$

其中，$B_i(x_1,\cdots x_k)$，$(i=0,1,\cdots,n)\in F[x_1,\cdots x_k]$，且每个$B_i$中$x_j$的次数$<q$，$B_n(x_1\cdots,x_k)\neq 0$。$n<q$。

由归纳假设，∵$B_n(x_1,\cdots x_k)$是$F[x_1\cdots x_k]$中非零多项式，且其中每个x_i的次数<F的元q数，∴在F中存在$c_1,\cdots,c_k$。使$B_n(c_1,\cdots,c_k)\neq 0$，于是，多项式

$$f(c_1,\cdots c_k,x_{k+1})=B_0(c_1,\cdots,c_k)+B_1(c_1,\cdots,c_k)x_{k+1}+\cdots,+B_n(c_1,\cdots,c_k)x_{k+1}^n$$

是$F[x_{k+1}]$中n次的非零多项式，根据定理7，最多只有n个的c'_{k+1}使$f(c_1,\cdots c_k,c'_{k+1})=0$，而∵$n<$F的元数q，∴F中必有一元$c_{k+1}$，使$f(c_1,c_1,\cdots,c_{k+1})\neq 0$

由归纳法原理，命题对所有自然数 成立。

下面各题里的F都与第2题的F相同。

3.求证：每个r变元（$\widetilde{F}^{(r)}$的元素）函数是一个多项函数（提示：枚列函数的集合及多项函数的集合）。

〔证法一〕：令$\widetilde{F}^{(r)}=(F, F^{(r)})=\{f:(s_1,\cdots,s_r)\to f(s_1,\cdots,s_r)\in F, s_1,\cdots,s_r\in F\}$
并考虑多项函数的集合：$F[s_1,\cdots s_r]=$

$\{\sum a_{i_1\cdots i_r}s_1^{i_1}\cdots s_r^{i_r}|a_{i_1\cdots i_r}\in F, i_1,\cdots, i_r$
$<$F的元数q$\}$显然$F[s_1,\cdots s_r]\leqslant F[x_1,\cdots x_r]$

∵F的元数为q，每个S_i在F中都可取q个值，所以
$F^{(r)}=\{(s_1,\cdots,s_r)|s_1,\cdots,s_r\in F\}$的元数为$q^r$，又∵
$\widetilde{F}^{(r)}$中元是$F^{(r)}$到F的单值映照，对每个$(s_1,\cdots,s_r)$都有q个这样的映照，∴$\widetilde{F}^{(r)}$的元数为q^{q^r}。

同样，考虑$F[s_1,\cdots,s_r]$的元数。∵$i_1,\cdots,i_r<q$，∴每个i_k都有q个取值：$i_k=0, 1,\cdots, q-1$，∴形如$s_1^{i_1}\cdots s_r^{i_r}$的单项式有$q^r$个，又∵它的系数$a_{i_1\cdots i_r}$是F中元，它又有q个取值，∴$F[s_1,\cdots,s_r]$的元素$q^{q^r}$，而且$F[s_1,\cdots,s_r]$中的多项函数都不相同。这是因为对于任意$f(x_1,\cdots,x_r)$，$g(x_1,\cdots,x_r)\in F[x_1,\cdots,x_r]$，$f\neq g$，则$f-g$是$F[x_1,\cdots,x_r]$中非零多项式，如果，$f,g\in F[s_1,\cdots,s_r]$，即它的所有$s_i$的指数$r_i$都$<q$，则由第2题知，存在$c_1,\cdots,c_r\in F$，使得$(f-g)(c_1,\cdots,c_r)\neq 0$，亦即$f-g$是$F[s_1,\cdots,s_r]$中非零多项函数，∴$f(s_1,\cdots,s_r)\neq g(s_1,\cdots,s_r)$。

∵$F[s_1,\cdots,s_r]$中的多项函数当然是r变元函数，∴$F[s_1,\cdots,s_r]\subseteq\widetilde{F}^{(r)}$但因$F[s_1,\cdots,s_r]$与$\widetilde{F}^{(r)}$所含元数

相同，$\therefore F(s_1, \cdots, s_r)=\overline{F}^{(r)}$，即证得每个r变元函数都是多项函数。

〔证法二〕：对r施行数学归纳法。当r＝1时，设f(s)为任一单元函数。

令F(s)＝

$$\sum_{i=1}^{q} f(a_i)\cdot\frac{(s-a_1)\cdots(s-a_{i-1})(s-a_{i+1})\cdots(s-a_q)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_q)}$$

则$F(a_i)=f(a_i)$，$i=1, 2, \cdots, q$。$\therefore F(s)=f(s)$，即f(s)为多项函数。

归纳假设$r=k-1$时，命题成立。则当$r=k$时，设$f(s_1,\cdots, s_k)$为任一k变元函数。

$$令F(s_1, \cdots, x_k)=\sum_{i=1}^{q} f(s_1, \cdots, s_{k-1}, a_i)$$

$$\frac{(s_k-a_1)\cdots(s_k-a_{i-1})(s_k-a_{i+1})\cdots(s_k-a_q)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_q)}$$ 由归纳假设知$f(s_1, \cdots, s_{k-1}, a_i)$，($i=1, 2, \cdots, q$) 都是多项函数，故$F(s_1, \cdots, s_k)$为多项函数，又任意$(c_1, \cdots, s_k)\in\overline{F}^{(k)}$，$F(c_1, \cdots, c_k)=f(c_1,\cdots,c_k)$，$\therefore F(s_1,\cdots, c_k)=f(s_1, \cdots, s_k)$，即$f(s_1, \cdots, s_k)$为多项函数。命题成立。

4．验证：$F[x_1, x_2, \cdots, x_r]$里任一个多项式可写成形状

$$\sum_{i=1}^{r} g_i(x_1, x_2, \cdots, x_r)(x_i^q-x_i)+g_0(x_1, x_2, \cdots, x_r)$$

这里g_0对于每个x_i的次数$<q$

〔证〕：对r施行数学归纳法：

当r＝1时，由带余除法，F〔x〕中任一多项式f(x)可表为

$$f(x)=g(x)(x^q-x)+g_0(x)$$

其中$\deg g_0(x)<q$命题成立。

设对$r\leqslant k$命题成立。对任意$f(x_1,\cdots x_k,x_{k+1})\in F[x_1,\cdots,x_{k+1}]$，把$f(x_1,\cdots,x_k,x_{k+1})$写成：

$$f(x_1,\cdots,x_k,x_{k+1})=B_0(x_1,\cdots,x_k)+B_1(x_1,\cdots,x_k)x_{k+1}+\cdots+B_n(x_1,\cdots x_k)x_{k+1}^n$$

其中$B_i(x_1,\cdots x_k)\in F[x_1,\cdots x_k]$，$i=1\cdots,n$

由归纳假设，每个$B_i(x_1,\cdots x_k)$都可表为

$$B_i(x_1,\cdots,x_k)=\sum_{j=1}^{k}g_{ij}(x_1,\cdots,x_k)(x_i^{q}-x_j)+g_{i0}(x_1\cdots,x_k)$$

这里g_{i0}对于$x_1,\cdots,x_k$的次数$<q$

$$\therefore f(x_1\cdots,x_k,x_{k+1})=\sum_{i=0}^{n}\left(\sum_{j=0}^{k}g_{ij}(x_1\cdots,x_k)(x_j^q-x_j)+g_{i0}(x_1,\cdots x_k)\right)x_{k+1}^i$$

$$=\sum_{i=0}^{n}\left(\sum_{j=1}^{k}g_{ij}(x_1,\cdots,x_k)(x_j^q-x_j)\right)x_{k+1}^i+\sum_{i=0}^{n}g_{i0}(x_1,\cdots x_k)x_{k+1}^i$$

$$=\sum_{j=1}^{k}\left(\sum_{j=0}^{n}g_{ij}(x_1\cdots,x_k)x_{k+1}^i\right)(x_j^q-x_j)+$$

$$\sum_{i=0}^{n} g_{i0}(x_1, \cdots, x_k) x_{k+1}^{i}$$

由带余除法，$\sum_{i=0}^{n} g_{i0}(x_1,\cdots,x_k) x_{k+1}^{i} \in F[x_1, \cdots x_k]$

可表为

$$\sum_{i=0}^{n} g_{i0}(x_1, \cdots x_k) x_{k+1}^{i} = g_k(x_1 \cdots x_k, x_{k+1})(x_{k+1}^{q} - x_{k+1}) + g_0(x_1, \cdots, x_k, x_{k+1})$$

其中，$g_0(x_1, \cdots, x_k, x_{k+1})$关于$x_{+1}$的次数$<q$，又∵它是通过带余除法从$g_{i0}(x_1, \cdots, x_k)$中得来，∴它关于$x_1, \cdots, x_k$的次数$<q$

∴$g_0(x_1, \cdots, x_k, x_{k+1})$关于$x_1, \cdots x_k, x_{k+1}$的次数$<q$。

记$g_j(x_1, \cdots, x_k, x_{k+1}) = \sum_{i=0}^{n} g_{ij}(x_1, \cdots x_k) x_{k+1}^{i}$，则

$$f(x_1, \cdots, x_k, x_{k+1}) = \sum_{j=1}^{k} g_j(x_1 \cdots, x_k, x_{k+1})(x_j^q - x_j) + g_k(x_1 \cdots x_k, x_{k+1})(x_{k+1}^{q} - x_{k+1}) + g_0(x_1 \cdots x_k, x_{k+1})$$

$$= \sum_{j=1}^{k+1} g_j(x_1, \cdots x_k, x_{k+1})(x_j^q - x_j) + g_0(x_1, \cdots x_k, x_{k+1})$$

∴当$r = k+1$时命题成立。于是由归纳法原理，对于任

意自然数r，命题都成立。

5．求证：如果$m(x_1,x_2,\cdots,x_r)$是一个多项式，使函数$m(s_1,s_2,\cdots s_r)=0$，则$m(x_1,x_2,\cdots,x_r)$可写成形状

$$\sum g_j(x_1,x_2,\cdots x_r)(x_i^q-x_i)$$

〔证〕：由第4题，$m(x_1,x_2,\cdots,x_r)$可写成

$$m(x_1,x_2,\cdots,x_r)=\sum_{i=1}^{r} g_i(x_1,x_2,\cdots x_r)(x_i^q-x_i)+g_0(x_1,x_2,\cdots,x_r),$$

其中g_0中$x_1,x_2\cdots,x_r$的次数都$<p$因为对任意$s_1,s_2,\cdots,s_r\in F$，$m(s_1,s_2,\cdots,s_r)=0$，$s_i^q-s_i=0$，

$\therefore g_0(s_1,s_2,\cdots s_r)=m(s_1,s_2,\cdots,s_r)=0$。由此推知$g_0(x_1,x_2,\cdots x_r)=0$，因为如果$g_0(x_1,x_2,\cdots,x_r)\neq 0$，它对于$x_1,x_2,\cdots,x_r$的次数都$<q$，由第2题知，在F里存在$c_1,\cdots,c_r$使$g_0(c_1,c_2,\cdots,c_r)\neq 0$即$g_0(s_1,s_2,\cdots,s_r)$不是零函数，这就得出矛盾。

$\therefore m(x_1,x_2,\cdots,x_r)=\sum g_i(x_1,x_2,\cdots,x_r)(x_i^q-x_i)$

6．令$f(x_1,x_2,\cdots,x_r)$是一个多项式，使$f(0,0,\cdots,0)=0$，并且对于所有$(c_1,c_2,\cdots,c_r)\neq(0,0,\cdots,0)$都有

$$f(c_1,c_2,\cdots c_r)\neq 0$$

求证：如果$F(x_1,x_2,\cdots,x_r)=1-f(x_1,x_2,\cdots,x_r)^{q-1}$则当$(c_1,c_2,\cdots c_r)=(0,0,\cdots,0)$时$F(c_1,c_2,\cdots,c_r)=1$，在其他情形时，$F(c_1,c_2,\cdots,c_r)=0$（这里q是有限域F的元数）

〔证〕：当$(c_1,c_2,\cdots,c_r)=(0,0,\cdots,0)$时，

$f(0, 0, \cdots 0) = 0$

$$f(0, 0, \cdots, 0)^{q-1} = 0^{q-1} = 0$$

$\therefore F(c, c_2, \cdots, c_r) = F(0, 0\cdots, 0) = 1 - f(0, 0, \cdots, 0)^{q-1} = 1 - 0 = 1$

当 $(c_1, c_2, \cdots, c_r) \neq (0, 0, \cdots, 0)$ 时，$f(c_1, c_2, \cdots, c_r) \neq 0$

$\therefore f(c_1, c_2, \cdots, c_r) \neq (0, 0, \cdots, 0)$ 时，$f(c_1, c_2, \cdots, c_r) \neq 0$

$\therefore f(c_1, c_2, \cdots, c_r)$ 是F中非零元，F的非零元全体构成乘群的元数为q-1，根据Lagrange定理，即得

$$f(c_1, c_2, \cdots c_r)^{q-1} = 1$$

$\therefore$ 此时有 $F(c_1, c_2, \cdots, c_r) = 1 - f(c_1, c_2, \cdots, c_r)^{p-1} = 1 - 1 = 0$

7．验证：第6题的F与

$$F_0 = (1 - x_1^{q-1})(1 - x_2^{q-1})\cdots(1 - x_r^{q-1})$$

决定同一函数，于是证明：$\deg F \geqslant r(q-1)$（这里，$\deg F$ = F的总次数）

〔证〕：当 $(c_1, \cdots, c_r) = (0, \cdots, 0)$ 时，

$F_0(0, \cdots, 0) = (1 - 0^{q-1})(1 - 0^{q-1})\cdots(1 - 0^{q-1}) = 1 = F(0, \cdots, 0)$

当 $(c_1, \cdots, c_r) \neq (0, \cdots, 0)$ 则至少有一个 $c_i \neq 0$

$\therefore c_i^{q-1} = 1$，即 $1 - c_i^{q-1} = 0$

$\therefore F_0(c_1, \cdots, c_i, \cdots c_r) = (1 - c_1^{q-1})\cdots(1 - c_i^{q-1})(1 - c_r^{q-1}) = 0 = F(c_1, \cdots c_i, \cdots c_r)$

因此F与F_0决定同一函数。

考察多项函数 $F(x_1, \cdots x_r) - F_0(x_1, \cdots, x_r)$，$\because$ F与

F_0决定同一函数，∴ $F-F_0$为零函数，即对任意$s_1,\cdots,s_r\in F$

$$F(s_1\cdots, s_r)-F_0(s_1, \cdots, s_r)=0$$

由第五题可得

$$F(x_1, \cdots, x_r)-F_0(x_1,\cdots x_r)=\sum_{i=1}^{r} g_i(x_1,\cdots,$$

$$x_r)(x_i^q-x_i)$$

即$F(x_1, \cdots, x_r)=\sum g_i(x_1, \cdots, x_r)(x_i^q-x_i)$ $+F_0(x_1, \cdots, x_r)$

因为$F_0(x_1,\cdots,x_r)$的首项为$x_1^{q-1}\cdots x_r^{q-1}$，∴ $\deg F_0=r(q-1)$如果$\sum g_i(x_1, \cdots, x_r)(x_i^q-x_i)$不含有$x_1^{q-1}\cdots x_r^{q-1}$的项则$F(x_1, \cdots x_r)$含有$x_1^{q-1}\cdots x_r^{q-1}$，∴ $\deg F\geqslant r(q-1)$如果$\sum g_i(x_1, \cdots, x_r)$含有$x_1^{q-1}\cdots x_r^{q-1}$而与$F_0$中相同的项相消，则它必须含有$(x_1^{q-1}x_2^{q-1}\cdots x_i^{q-2}\cdots x_r^{q-1})(x_i^q-x_i)$即它含有$x_1^{q-1}\cdots x_r^{q-1}$，同时也含有$x_1^{q-1}x_2^{q-1}\cdots x_i^{2q-2}\cdots x_r^{q-1}$，而这后一项的总次数$\geq r(p-1)$，∴这时亦有$\deg F\geq r(q-1)$

8．求证：阿廷—捷发莱（Artin-Chevalley）定理：

令$f(x_1, x_2, \cdots x_r)$是$n(<r)$次多项式，并设

$$f(0, 0, \cdots, 0)=0$$

则有一个$(c_1, c_2, \cdots, c_r)\neq(0, 0, \cdots, 0)$存在，使$f(c_1, c_2, \cdots, c_r)=0$

〔证〕：反证法。如果对所有$(c_1, c_2\cdots, c_r)\neq(0, 0, \cdots, 0)$都有$f(c_1, c_2, \cdots, c_r)\neq 0$，则由第6，第7题的结果

令$F(x_2, x_1, \cdots x_r)=1-f(x_1, x_2, \cdots, x_r)^{q-1}$

有$\deg F \geqslant r(q-1)$，即$\deg f(x_1, x_2, \cdots x_i)^{q-1} \geqslant r(q-1)$

$\therefore \deg f(x_1, x_2, \cdots, x_r) \geqslant r$，这与假设$f(x_1, x_2, \cdots, x_r)$是小于r次的多项式矛盾，因此必存在$(c_1, c_2, \cdots, c_r) \neq (0, 0, \cdots, 0)$使得$f(c_1, c_2, \cdots, c_r) = 0$

第四章　因子分解的初等理论

习　题　46

1. 验证：$I[\sqrt{-5}]$适合A.

〔证〕：$I[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n是整数\}$

设$a_1, a_2, \cdots, a_i, a_{i+1}, \cdots$，是$I[\sqrt{-5}]$中一列元，其中每个$a_{i+1}$是$a_i$的真因子，于是有

$a_i = a_{i+1}b$，其中b不是单位元

$\because I[\sqrt{-5}]$中单位元是± 1，$\therefore b \neq \pm 1$，$\therefore N(b) > 1$

而$\because N(a_i) = N(a_{i+1}b) = N(a_{i+1})N(b)$

$\therefore N(a_i) > N(a_{i+1})$，$i = 1, 2, \cdots$，即

$N(a_1) > N(a_2) > \cdots > N(a_i) > N(a_{i+1}) > \cdots$

$\because N(a_1)$是一个有限正整数，而每一个$N(a_i)$也都是正整数，那么比(Na_1)小的正整数只能有有限个，所以必定存在某正整数k，使得当$n > k$时$a_n = a_k$，也就是说在$I[\sqrt{-5}]$中只能有有限序列$a_1, a_2, \cdots a_k$，使每个a_{i+1}是a_i的真因子。

2. 令A是$a_1x^{\alpha_1} + a_2x^{\alpha_2} + \cdots + a_nx^{\alpha_n}$的集合，这里$a_i$是域F里任意元素，而$\alpha_i$是非负的有理数，依普通方式定义加法，并以$x^{\alpha}x^{\beta} = x^{\alpha+\beta}$定义乘法。验证：A是带恒等

元素的一个交换整区；并验证：A的元素 x 不是一个单位元素，但这元素不能分解为不可约元素。

〔证〕：设 $A=\{a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n}\mid a_i\in$ 域F，α_i为非负有理数，n为任意整正数 $\}$ 任取 $a=\sum_{i=1}^{n}a_ix^{\alpha_i}$，

$b=\sum_{j=1}^{m}b_jx^{\beta_j}$，$c=\sum_{k=1}^{l}c_kx^{r_k}\in A$

∵在A中加法是按通常形式定义，所以关于加法显然是封闭的，且满足加法的交换律与结合律，即

1）$a+b\in A$，2）$a+b=b+a$，3）$(a+b)+c=a+(b+c)$，4）$0=0x^{\alpha_1}+0x^{\alpha_2}+\cdots+0x^{\alpha_n}$是A的零元：$0+a=a+0=0$，5）$-a=-a_1x^{\alpha_1}-a_2x^{\alpha_2}-\cdots-a_nx^{\alpha_n}\in A$是a的负元：

$$a+(-a)=(-a)+a=0$$

6）$a\cdot b=(\sum_{i=1}^{n}a_ix^{\alpha_i})(\sum_{j=1}^{m}b_jx^{\beta_j})=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_jx^{\alpha_i+\beta_j}\in A$

且，$ab=\sum\sum a_ib_jx^{\alpha_i\beta_j}=\sum\sum b_j\cdot a_ix^{\alpha_i+\beta_j}=ba$

A关于乘法封闭，且可交换。

7）∵F是域，F中元素a_i，b_j，c_k关于乘法满足结合律。

$$\therefore (ab)c=\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{k}(a_ib_j)c_kx^{(\alpha_i+\beta_j)+r_k}$$

$$=\sum_i\sum_j\sum_k a_i(b_jc_k)x^{\alpha_i+(\beta_j+r_k)}=a\cdot(bc)$$

∴ A满足关于乘法的结合律

8）$(a+b)c=(\sum_{i=1}^{n}a_i x^{\alpha_i}+\sum_{j=1}^{m}b_j x^{\beta_j})\circ(\sum_{k=1}^{l}c_k x^{r_k}$

$$=\sum_{i=1}^{n}\sum_{k=1}^{l} a_i c_k x^{\alpha_i+r_k}+\sum_{j=1}^{m}\sum_{k=1}^{l} b_j c_k x^{\beta_j+r_k}$$

$$=ac+bc$$

∴A满足乘法对加法的分配律

9）$1\cdot x^{\circ}=1\in A$是A的恒等元：$(\sum a_i x^{\alpha_i})(1\cdot x^{\circ})=\sum a_i x^{\alpha_i}$

10）设$a=\sum_{i=1}^{n}a_i x^{\alpha_i}\neq 0$，则至少有一个$a_{i_0}\neq 0$

而$ab=(\sum_{i=1}^{n}a_i x^{\alpha})(\sum_{j=1}^{m}b_j x^{\beta_j}=\sum_{i=1}^{n}\sum_{j=1}^{m}a_i b_j x^{\alpha_i+\beta_j}=0$

则对所有的a_i，b_j，均有$a_i b_j=0$，特别$a_{i_0}b_j=0$

∵a_{i_0}，$b_j\in$域F，F中无零因子，∴$b_j=0$，$j=1$，2，…，m

$$∴b=\sum_{j=1}^{m}b_j x^{\beta_j}=0$$

∴A中亦无非零的零因子。

综上所述，A是一个带恒等元的交换整区。

其次证明x不是一个单位元素，且不能分解为不可约元素的积。

定义$f(x)=a_1x^{\alpha_1}+a_2x^{\alpha_2}+\cdots+a_nx^{\alpha_n}$的次数

$\deg f(x)=\max\{\alpha_i\}$，$\deg 0=-\infty$。

显然有$\deg[f(x)g(x)]=\deg f(x)+\deg g(x)$

若 x 是A的单位元素，即存在 $f(x)\in A$，使 $xf(x)=1$，于是 $\deg x+\deg f(x)=\deg 1=0$，得出 $\deg f(x)=-1$，此不可能，故 x 不是A的单位元素。

又 x，$x^{1/2}$，$x^{1/3}$，…，$x^{1/n}$，…，是一个以 x 为开头的无限序列，且每一项是它的前一项的真因子，即A不满足因子链条件。因而 x 不能分解为不可约元素的积。

3.验证：条件B在任一个高斯半群里成立。

〔证〕：设s是高斯半群，p是s的不可约元，且 $p\mid ab$，a,b是s中任意二个元，a,b,不可能都是单位元，因为如果a,b都是单位元，则ab是单位元，∴p也是单位元，这与p是不可约元的假设矛盾。

当a,b中有一个（不妨设b）是单位元。∵$p\mid ab$，∴s中存在c，使 $pc=ab$，$p(cb^{-1})=a$，∴$p\mid a$，因此这时条件B成立。

若a,b都不是单位元，则由 $pc=ab$ 知c也不是单位元，（∵如果c也是单位元，则有 $c^{-1}\in s$ 使得 $cc^{-1}=1$，∴$p=abc^{-1}$ 于是得出a,b是p的真因子，这与p不可约矛盾）因此可把a,b,c作不可约元的分解：

$a=p_1\cdots p_k$，$b=p_{k+1}\cdots p_l$，$c=p_1'\cdots p_t'$

其中 p_1，…，p_k，p_{k+1}，…，p_l，以及 p_1'，…，p_t' 都是s的不可约元，于是有 $pp_1'\cdots p_t'=p_1\cdots p_kp_{k+1}\cdots p_l$

∵s是高斯半群，在其中任一非单位元的不可约元分解在实质上是唯一的，∴在 p_1，…，p_k，p_{k+1}，…，p_l 中必有一元 p_i，使得 $p\sim p_i$，即 $p\mid p_i$，若 p_i 是 p_1，…，p_k 中的一个，则 $p\mid a$，若 p_i 是 p_{k+1}，…，p_l 中的一个，则 $p\mid b$，即p是s的元素，于是条件B成立。

习　题　47

1. 如果元素m对于元素a,b具有$a|m$，$b|m$，并且适合$a|n$，$b|n$的任一个元素n一定有$m|n$，则m叫做a及b的最小公倍（简写作l·c·m），求证：高斯半群里任意二个元素有一个l·c·m。

〔证法一〕设s是高斯半群，a,b是s中任二个元素：

若a,b都是s的单位元，则l·c·m{a,b}～1

若a,b中有一个（设为b）是s的单位元，则l·c·m{a,b}～a

若a,b都不是s的单位元，则可把a,b在s中作相同的不可约元分解：$a=up_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}$，$b=vp_1^{j_1}p_2^{j_2}\cdots p_k^{j_k}$

其中p_1，…，p_k是 的不可约元，且两两不相伴，i_1，i_2，…，i_k；j_1，j_2，…，$j_k\geqslant 0$，u,v是s的单位元素，今取元素$m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$，其中$e_l=\max\{i_l, j_l\}$，$l=1$，…，k，显然有$a|m$，$b|m$。设任一元素n满足$a|n$，$b|n$，则在n的分解式$n=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}\cdots p_q^{f_q}$中，每一个$f_l\geqslant i_l$，$f_l\geqslant j_l$，$\therefore f_l\geqslant\max\{i_l, j_l\}=l_l$，$\therefore m|n$，

因此，$m=p_1^{e_1}q_2^{e_2}\cdots p_k^{e_k}$就是一个l·c·m{a,b}

〔证法二〕因为高斯半群里的任二个元都有最大公因子，可设$(a,b)=d$，$a=a_1d$，$b=b_1d$，$(a_1,b_2)\sim 1$，则a_1b_1d就是a,b的一个l·c·m。事实上，显然$a|a_1b_1d$，$b|a_1b_1d$若有n使得$a|n$且$b|n$，则$a_1b_1d|nb_1$，$a_1b_1d|na_1$，

$\therefore a_1b_1d|(nb_1,na_1)$，但$\because(a_1, b_1)\sim 1$，$\therefore(n_1a,nb_1)\sim n(a_1,b_1)\sim n$，$\therefore a_1b_1d|n$，故$a_1b_1d$是a,b的一个最小公倍。

2. 如果s是高斯整区，令[a,b]表a及b的一个l·c·m。

求证：$(a,b)[a,b]\sim ab$，并证：$[a,(b,c)]=([a,b],[a,c])$

〔证〕：（1）设$a=up_1^{i_1}\cdots p_k^{i_k}$，$b=vp_1^{j_1}\cdots p_k^{j_k}$ ∵ a，b 的任意两个l·c·m都相伴，∴由上题$[a,b]\sim p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ $e_l=\max\{i_l,j_l\}$，$(a,b)\sim p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$，$f_l=\min\{i_l,j_l\}$

$$\therefore (a,b)[a,b]\sim p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}\cdot p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$
$$=p_1^{f_1+e_1}p_2^{f_2+e_2}\cdots p_k^{f_k+e_k}=p_1^{i_1+j_1}p_2^{i_2+j_2}\cdots$$
$$p_k^{i_k+j_k}=(p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k})(p_1^{j_1}p_2^{j_2}\cdots p_k^{j_k})\sim ab$$

（2）又设$c=\lambda p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，则

$$(b,c)=p_1^{\min\{j_1,r_1\}}p_2^{\min\{j_2,r_2\}}\cdots p_k^{\min\{j_k,r_k\}}$$

$$\therefore [a,(b,c)]=p_1^{\max\{i_1,\min\{j_1,r_1\}\}}p_2^{\max\{i_2,\min\{j_2,r_2\}\}}\cdots p_k^{\max\{i_k,\min\{j_k,r_k\}\}}$$

同理，$$([a,b],[a,c])=p_1^{\min\{\max\{i_1,j_1\}\max\{i_1,r_1\}\}}\cdots p_k^{\min\{\max\{i_k,j_k\},\max\{i_k,r_k\}\}}$$

比较$[a,(b,c)]$及$([a,b],[a,c])$中p_l的指数（$l=1,\cdots,k$）

$M=\max\{i_l,\min\{j_l,r_l\}\}$，与$N=\min\{\max\{i_l,j_l\},\max\{i_l,r_k\}\}$

i_l，j_l，r_l之间关系有下列几种情况：

①$i_l\geqslant j_l\geqslant r_l$②$i_l\geqslant r_l\geqslant j_l$③$j_l\geqslant i_l\geqslant r_l$④$j_l\geqslant r_l\geqslant i_l$
⑤$r_l\geqslant i_l\geqslant j_l$⑥$r_l\geqslant j_l\geqslant i_l$

在情况①时，$M=i_l$，$N=i_l$

在情况②时，$M=i_l$，$N=i_l$

在情况③时，$M=i_l$，$N=i_l$

在情况④时，$M=r_i$，$N=r_i$

在情况⑤时，$M=i_l$，$N=i_l$

在情况⑥时，$M=j_l$，$N=j_l$

∴对所有情形均有$M=N$

因此$[a,(b,c)]=([a,b],[a,c])$

3.如果p是一个正素数，求证：二项式系数

$$C^i_p=\frac{p!}{i!\ (p-i)!}\ (1\leqslant i\leqslant p-1)$$

可被p整除，由此证明：特征数是p的任一个交换整区里，对于所有a及b，$(a+b)^p=a^p+b^p$成立。

〔证〕：∵ $c^i_p=\frac{p!}{i!\ (p-i)!}$，∴$p!=c^i_p\cdot i!\ (p-i)!$

又$p\mid p!$，∴$p\mid c^i_p\cdot i!\ (p-i)!$

∵p是素数，∴必有$p\mid c^i_p$或$p\mid i!\ (p-i)!$

但∵$i<p$，∴$p\nmid i!\ (p-i)!$ 从而$p\mid c^i_p$

∵$(a+b)^p=a^p+c^1_pa^{p-1}b+\cdots+c_p^{p-1}ab^{p-1}+b^p$

而$p\mid c^i_p$，即$c^i_p\equiv 0\ (\mathrm{mod}\,p)$，$i=1,\ 2,\ \cdots,\ p-1$

∴$c^i_pa^{p-i}b^i=0$，$i=1,\ 2,\ \cdots,\ p-1$

因此$(a+b)^p=a^p+b^p$

4.正整数的默比乌斯(Mobius)函数u(n)定义为

1）$u(1)=1$，2）如果n有平方因子，则$u(n)=0$，3）如果n不含有平方因子，而s是n的长，则$u(n)=(-1)^s$

求证：u(n)是乘法函数，亦即：如果$(n_1,\ n_2)=1$，则$u(n_1n_2)=u(n_1)u(n_2)$；并证

$$\sum_{d\mid n}u(d)=\begin{cases}1\ (n=1\text{时})\\0\ (n>1\text{时})\end{cases}$$

〔证〕：（1）若n_1，n_2中有一个（不妨设n_1）是1，则$u(n_1n_1)=u(n_2)$，$u(n_1)u(n_2)=u(n_2)$，∴$u(n_1n_2)=u(n_1)(n_2)$。若n_1，n_2中有一个含有平方因子，则n_1n_2也含有平方因子，此时$u(n_1n_2)=0=u(n_1)u(n_2)$

现假定n_1，n_2都大于1，且都不含平方因子，设

$$n_1=p_1p_2\cdots p_n,\quad n_2=p_1'p_2'\cdots p_m'$$

其中p_1，…，p_n两两不相伴，p_1'，…，p_m'也两两不相伴$n_1n_2=p_1p_2\cdots p_np_1'p_2'\cdots p_m'$

∵$(n_1, n_2)=1$，∴每个p_i与每个p_j'也都不相伴

∴$n+m$就是n_1n_2的长度，从而

$$u(n_1n_2)=(-1)^{n+m}=(-1)^n\cdot(-1)^m=u(n_1)u(n_2)$$

（2）设$n'=p_1^{t_1}p_2^{t_2}\cdots p_s^{t_s}$，考察满足$d\mid n'$的d.若$u(d)=0$，则d含有平方因子，若$u(d)\neq 0$，则d不含有平方因子，所以我们只须对$n=p_1p_2\cdots p_s$考虑因子d。

当$n=1$时，则

$$\sum_{d\mid n}u(d)=\sum_{d\mid 1}u(d)=u(1)=1$$

当$n>1$时，$n=p_1p_2\cdots p_s$的因子d的个数为

$$1+c^1{}_s+c^2{}_s+\cdots+c^s{}_s=(1+1)^s=2^s$$

长度为k的因子d的个数为$c^k{}_s$

$$\therefore\sum_{d\mid n}u(d)=\sum_{k=0}^{s}c^k{}_s(-1)^k=1-c^1{}_s+c^2{}_s-\cdots+(-1)^sc^s{}_s=(1-1)^s=0$$

5.证明：默比乌斯反演公式：如果f(n)是正整数的一个函数，其值属于一个环里，并且

$$g(n)=\sum_{d|n}f(d)$$

则 $$f(n)=\sum_{d|n}u\left(\frac{n}{d}\right)g(d)$$

证：当$n=1$时，$\sum\limits_{d|1}u\left(\frac{1}{d}\right)g(d)=u(1/1)g(1)$

$$=u(1)g(1)=g(1)=\sum_{d|1}f(d)=f(1)$$

现设$n>1$，d取遍n的所有因子，而$t|d$，则t亦可取遍n的所有因子，且$\frac{n}{d}\Big|\frac{n}{t}$

$$\sum_{d|n}u\left(\frac{n}{d}\right)g(d)=\sum_{d|n}u\left(\frac{n}{d}\right)\left[\sum_{t|d}f(t)\right]$$

$$=\sum_{d|n}\sum_{t|d}u\left(\frac{n}{d}\right)f(t)=\sum_{t|n}\sum_{\frac{n}{d}|\frac{n}{t}}u\left(\frac{n}{d}\right)f(t)$$

$$=\sum_{t|n}\left[\sum_{\frac{n}{d}|\frac{u}{t}}\left(\frac{n}{d}\right)\right]f(t)\cdots(*)$$

由上题默比乌斯函数性质知

当$\frac{n}{t}>1$时，$\sum\limits_{\frac{n}{d}|\frac{n}{t}}u\left(\frac{n}{d}\right)=0$

当$\frac{n}{t}=1$时，即$t=n$时，$\sum\limits_{\frac{n}{d}|\frac{n}{t}}u\left(\frac{n}{d}\right)=1$

∴上式$(*)=f(t)\big|_{t=n}=f(n)$

即证得$f(n)=\sum_{d\mid n} u\left(\frac{n}{d}\right)g(d)$

6.如果$\varphi(n)$是欧拉φ函数，求证：

$$\varphi(n)=\sum_{d\mid n} u\left(\frac{n}{d}\right)d$$

（参看习题13第3题）

〔证〕：考察 $\sum_{d\mid(k,n)} u(d)$，$1\leqslant k\leqslant n$

由默比乌斯函数性质，若$(k,n)=1$，则 $\sum_{d\mid(k,n)} u(d)=1$

若$(k,n)>1$，则 $\sum_{d\mid(k,n)} u(d)=0$

因而有 $\sum_{d\mid(1,n)} u(d)+\sum_{d\mid(2,n)} u(d)+\cdots+\sum_{d\mid(n-1,n)} u(d)+\sum_{d\mid(n,n)} u(d)$

$$=\sum_{i=1}^{n}\sum_{d\mid(i,n)} u(d)=\varphi(n)$$

$\because d\mid(i,n)$，$\therefore d\mid i$且$d\mid n$

设n的所有因子是d_1，d_2，…，d_k，则把上式按$u(d_1)$，$u(d_2)$，…，$u(d_k)$重新组合，含$u(d_i)$的项共有$\frac{n}{d_i}$个

$$\therefore\sum_{i=1}^{n}\sum_{d\mid(i,n)} u(d)=\sum_{i=1}^{k} u(d_i)\cdot\frac{n}{d_i}$$

令$t_i=\frac{n}{d_i}$，则$d_i=\frac{n}{t_i}$，$t_i\mid n$且t_i取遍n的所有因子。

$$\therefore \sum_{i=1}^{k} u(d_i)\frac{n}{d_i} = \sum_{i=1}^{k} u\left(\frac{n}{t_i}\right)t_i = \sum_{d\mid n} u\left(\frac{n}{d}\right)d$$

$$\therefore \varphi(n) = \sum_{d\mid n} u\left(\frac{n}{d}\right)d$$

习　　题　48

1.求证：交换整区A的一个元素p是一个素元，必须而且只须A/(p)是一个整区。

〔证〕：必要性。设$\bar{a}=a+(p)$与$\bar{b}=b+(p)$是A/(p)中两个元，并且$\bar{a}\cdot\bar{b}=ab+(p)=\bar{0}$，$\therefore p\mid ab$，$\because$p是素元，$\therefore p\mid a$或$p\mid b$，从而$\bar{a}=a+(p)=\bar{0}$或$\bar{b}==b+(p)=\bar{0}$，$\therefore$ A/(p)中没有非零的零因子，即A/(p)是整区。

充分性，设$p\mid ba$，则$\overline{ab}=\bar{a}\,\bar{b}=\bar{0}$

$\because$ A/(p)是整区，$\therefore \bar{a}=\bar{0}$或$\bar{b}=\bar{0}$，因此$p\mid a$或$p\mid b$即p是素元。

2.如果在一个主理想整区里，p是一个素元，求证：A/(p)是一个域。

〔证〕：由主理想整区定义知，A含有恒等元1，$\therefore$ A/(p)也含有恒等元$\bar{1}=1+(p)$。因为主理想整区是高斯整区，而高斯整区的素元都是不可约元，$\therefore$p是A的不可约元。

设$\bar{a}=a+(p)\neq 0$，则$p\nmid a$，$\therefore (p,a)\sim 1$，现要证A中存在b，使得$\bar{a}\,\bar{b}=\overline{ab}=\bar{1}$，考察由a及p生成的理想$(a)+(p)$，因为A是主理想整区，所以存在$d\in A$，使得$(a)+(p)=(d)$，$\because (a)\sqsubseteq(d)$，$(p)\sqsubseteq(d)$，$\therefore d\mid a$，$d\mid p$，即d是a与p的公因子，但$\because (p,a)\sim 1$

$\therefore d \sim 1$，$\therefore (a)+(p)=(d)=(1)=A$

因此特别对于$1\in A$，必有$b,c\in A$，使得

$$ab+pc=1$$
$$\overline{ab+pc}=\overline{ab}+\overline{pc}=\overline{ab}+\overline{0}=\bar{a}\bar{b}=\bar{1}$$

即$\bar{a}$是$A/(p)$的单位元，因而$A/(p)$是一个除环。又$\because$主理想整区A是可换环，所以$A/(p)$也是可换除环，即A/p是域

3. 令A是一个主理想整区，B是包括A的任一个交换整区。如果$a,b\in A$有最大公因子$d\in A$，验证：在B里d是a及b的一个最大公因子。

〔证〕：$\because$ A是主理想整区，而d是$a,b\in A$在A中的最大公因子，$\therefore (a)+(b)=(d)$，即存在$a',b'\in A$，使得

$aa'+bb'=d$。设d'是B中a,b的公因子，

则$d' \mid aa'+bb'$，$\therefore d' \mid d$，这说明d仍是B中a与b的最大公因子，因而命题得证。

4. 令F是含有q个元素的一个有限域，$N(r,q)$表$F[x]$里r次不可约多项式的个数，求决定$N(2,q)$及$N(3,q)$。

〔解〕：$a'x^2+b'x+c'=a'(x^2+a'^{-1}b'x+a'^{-1}c')$

$$\overset{令}{=}a'(x^2+bx+c)$$

$\because a'x^2+b'x+c' \sim x^2+bx+c$

$\therefore$在考虑决定形如$a'x^2+b'x+c'$的二次不可约多项式个数时，只须考虑决定形如x^2+bx+c的二次不可约多项式的个数。同样三次不可约多项式个数亦只须决定形如x^3+ax^2+bx+c的个数。

（1）考虑形如x^2+bx+c的多项式，$\because b,c$可取遍F的所

有q个元，∴形如x^2+bx+c的多项式共有q^2个。再考虑其中可约的个数，若x^2+bx+c可约，它必是如下形式

1）$x^2+bx+c=(x-a)^2$

2）$x^2+bx+c=(x-a_1)(x-a_2),a_1\neq a_2$

相伴的算同一个，则1）的情形有$c^1{}_q$种，2）的情形有$c^2{}_p$种，所以形如x^2+bx+c的可约多项式共$c^1{}_q+c^2{}_q=$ $q+\frac{q(q-1)}{2}$（个），因而不可约多项式就有$N(2,q)=q^2-(q+\frac{q(q-1)}{2})=\frac{q(q-1)}{2}$个。

（2）考虑形如x_3+bx^2+cx+d的多项式，这样的多项式共有q^3个，它若是可约，则必是如下形式：

1）$x^3+bx^2+cx+d=(x-a)^3$

2）$x^3+bx^2+cx+d=(x-a)(x^2+a_1x+a_2)$，其中$x^2+a_1x+a_2$不可约。

3）$x^3+bx^2+cx+d=(x-a_1)(x-a_2)(x-a_3)$，其中$a_1$，$a_2$，$a_3$不全相同。

1）的情形有$c^1{}_q$种，2）的情形有$c^1{}_qN(2,q)$种，3）的情形有$c^3{}_q+2c^2{}_q$种，所以形如x^3+bx^2+cx+d的可约多项式共有

$$c^1{}_q+c^1{}_qN(2,q)+c^3{}_q+2c^2{}_q=q+q\cdot\frac{q(q-1)}{2}+\frac{q(q-1)(q-2)}{3!}+2\cdot\frac{q(q-1)}{2!}=\frac{2q^3+q}{3}\text{（个）}$$

因此不可约多项式就有$N(3,q)==q^3-\frac{2q^3+q}{3}=$

$\frac{q(q+1)(q-1)}{3}$个$(q>2)$

当$q=2$时，$N(3,2)=2^3-[c^1{}_2+c^1{}_2N(2,2)+2c^2{}_2]$
$=2$

5.如果A是带恒等元素的一个交换整区，但不是域，求证：A〔x〕不是一个主理想整区。

〔证〕：∵A不是域，，∴A中必有非零元a，a不是A的单位元。考察由a及x生成的A〔x〕的理想。

$$(a)+(x)=\{af(x)+xg(x)\mid f(x),\ g(x)\in A[x]\}$$

$$=\{\sum_{i=0}^{n} a_i x^i \mid a\mid a_0\}$$

则(a)+(x)不是A〔x〕的主理想，事实上，如果(a)+(x)是A〔x〕的主理想，则必有$\sum_{j=0}^{k} a_j x^j\in A[x]$，使得

$$(a)+(x)=(\sum_{j=0}^{k} a_j x^j)$$

$\because a\in(a)\subseteq(\sum_{j=0}^{k} a_j x^j)$，∴必有$\sum_{i=0}^{m} b_i x^i\in A[x]$，使得

$a=\sum_{j=0}^{k} a_j x^j\cdot\sum_{i=0}^{m} b_i x^i$，比较两边得$a_1=\cdots=a_k=0$

且$a=a_0b_0$，即$a_0\mid a$，但$\because a\mid a_0$，$\therefore a\sim a_0$，$(a)=(a_0)$，$\therefore(a)+(x)=(a_0)=(a)$

$\because x\in(x)\subseteq(a)$，∴存在$\sum_{l=0}^{q} c_l x^l$，使得

$$x = a \cdot \sum_{l=0}^{q} c_l x^l$$，比较两边即有$ac_1 = 1$

从而a是单位元，这与假定矛盾。因此$(a)+(x)$不是$A[x]$的主理想，即$A[x]$不是主理想整区。

习　　题　　49

1．求证：形状如$m+n\sqrt{2}$的实数集合$I[\sqrt{2}]$是欧几里得整区，这里m,n是整数。

〔证〕：$I[\sqrt{2}]=\{m+n\sqrt{2} \mid m,n是整数\}$是实数域的子集，任取$a=m_1+n_1\sqrt{2}$，$b=m_2+n_2\sqrt{2}\in I[\sqrt{2}]$

$\because a-b=(m_1-m_2)+(n_1-n_2)\sqrt{2}\in I[\sqrt{2}]$

$ab=(m_1m_2+2n_1n_2)+(n_1m_2+n_2m_1)\sqrt{2}\in I[\sqrt{2}]$

$\therefore$ $I[\sqrt{2}]$构成实数域的一个子环，且$1+0\sqrt{2}\in I[\sqrt{2}]$是$I[\sqrt{2}]$的恒等元，而实数域满足交换律且无零因子，因此$I[\sqrt{2}]$是带有恒等元可换整区。

对于$a=m+n\sqrt{2}$，定义函数$\delta(a)=|m^2-2n^2|$，则它满足

1）显然$\delta(a)=|m^2-2n^2|\geqslant 0$，且$\delta(a)=0$必须且只须$m=n=0$，即$a=0$。

2）$\delta[(m_1+n_1\sqrt{2})(m_2+n_2\sqrt{2})]=\delta[(m_1m_2+2n_1n_2)+(m_1n_2+m_2n_1)\sqrt{2}]=|(m_1m_2+2n_1n_2)^2-2(m_1n_2+m_2n_1)^2|=|m_1^2m_2^2+4n_1^2n_2^2-2(n_1^2m_2^2+n_2^2n_1^2)|=|m_1^2-2n_1^2|\cdot|m_2^2-2n_2^2|$

$=\delta(m_1+n_1\sqrt{2})\delta(m_2+n_2\sqrt{2})$

3）对于任意$a=m_1+n_1\sqrt{2}$及$b=m_2+n_2\sqrt{2}\neq 0$令

$\frac{a}{b}=\frac{m_1+n_1\sqrt{2}}{m_2+n_2\sqrt{2}}=\alpha+\beta\sqrt{2}$，$\alpha$，$\beta$为有理数，则存在正整数m，n，使得$|m-\alpha|\leqslant\frac{1}{2}$，$|n-\beta|\leqslant\frac{1}{2}$。

$\therefore a=b(\alpha+\beta\sqrt{2})=b[(m+n\sqrt{2})+(\alpha-m)+(\beta-n)\sqrt{2}]=b(m+n\sqrt{2})+b[(\alpha-m)+(\beta-n)\sqrt{2}]\overset{记}{=}bq+\gamma$

$\because a, b(m+n\sqrt{2})\in I[\sqrt{2}]$

$\therefore \gamma=b[(\alpha-m)+(\beta-n)\sqrt{2}]=a-b(m+n\sqrt{2})\in I[\sqrt{2}]$

而且$\delta(\gamma)=\delta[b((a-m)+(\beta-n)\sqrt{2}]=\delta(b)\delta[(a-m)+(\beta-n)\sqrt{2}]$

$\because \delta[(a-m)+(\beta-n)\sqrt{2}]=|(a-m)^2-2(\beta-n)^2|\leqslant|(a-m)^2+2(\beta-n)^2|\leqslant(a-m)^2+2(\beta-n)^2\leqslant\frac{1}{4}+\frac{2}{4}=\frac{3}{4}<1$

$\therefore \delta(\gamma)=\delta[b((a-m)+(\beta-n)\sqrt{2})]<\delta(b)$

因此$I[\sqrt{2}]$是欧几里得整区。

2．令A是复数$m+n\sqrt{-3}$的全体，这里m及n或者都是整数，或者都是奇数的½，验证：A对于通常的加法及乘法成一个环，求证：A是欧几里得整区。

〔证〕：令$A=\{m+n\sqrt{-3}\mid m,n$或都是整数，或都是奇数的½$\}$，A是复数域的子集，任取$a=m_1+n_1\sqrt{-3}$，$b=m_2+n_2\sqrt{-3}$。（1）$a-b=(m_1-m_2)+(n_1-n_2)\sqrt{-3}\in A$（$\because$当$m_1, n_1$与$m_2, n_2$其中有一组是整数，而另一组是奇数的½，则$m_1-m_2$与$n_1-n_2$都是奇数的½）

$ab=(m_1m_2-3n_1n_2)+(m_1n_2+n_1m_2)\sqrt{-3}$

显然可以看出，不论那种情况，$m_1m_2-3n_1n_2$及$m_1n_2+n_1m_2$的分母最多是2，于是只须证明它们的差是整数就行。又$(m_1m_2-3n_1n_2)-(m_1n_2+n_1m_2)=m_1(m_2-n_2)-n_1(3n_2+m_2)$可以看出$m_2-n_2$，$3n_2+m_2$都是整数，由它们的差是偶数，于是它们必同为奇数或偶数，所以上式是整数，因而$m_1m_2-3n_1n_2$，$m_1n_2+n_1m_2$必同为整数或同为奇数的½。

$\therefore ab\in A$

由于A是复数域的子集合，且对减法、乘法封闭，故A是个子环，且是无零因子环。

（2）$1+0\sqrt{-3}=1\in A$，是A的恒等元。

显然在A中乘法交换律及相消律成立，所以A是带恒等元的可换整区。

（3）定义函数$\delta(m+n\sqrt{-3})=m^2+3n^2$

当m，n都是整数或都是奇数的½时，m^2+3n^2都是非负整数，直接验证可知

$\delta(a)=0\Leftrightarrow a=0$

而且$\delta(ab)=\delta(a)\delta(b)$

在上述所取a，b中，设$b\neq 0$

$\frac{a}{b}=\frac{m_1+n_1\sqrt{-3}}{m_2+n_2\sqrt{-3}}=\alpha+\beta\sqrt{-3}$，$\alpha$，$\beta$是有理数

可取到或都是整数，或都是奇数的½的u，v使得

$|\alpha-u|\leqslant\frac{1}{2}$，$|\beta-v|\leqslant\frac{1}{4}$

$a=b(\alpha+\beta\sqrt{-3})=b(u+v\sqrt{-3})+b[(\alpha-u)+$

记

$(\beta - v)\sqrt{-3}] = bq + \gamma$

$\because a, b(u + v\sqrt{-3}) \in A$, $\therefore \gamma = b[\alpha - u)$
$+ (\beta - v)\sqrt{-3}] = a - b(u + v\sqrt{-3}) \in A$

而且 $\delta(\gamma) = \delta(b)\delta[(\alpha - u) + (\beta - v)\sqrt{-3}]$

$= \delta(b)[(\alpha - u)^2 + 3(\beta - v)^2] \leqslant \delta(b)$.

$(\frac{1}{4} + \frac{3}{16}) = \delta(b) \cdot \frac{7}{16} < \delta(b)$.

$\therefore$ A是欧几里得整区。

3.求证：欧几里得整区里的一个元素a是单位元素必须而且只须 $\delta(a) = 1$

〔证〕：设A是欧几里得整区，$a \in A$

若a是A的单位元，则必存在 $b \in A$，使得 $ab = 1$

$\because$ 对于任意 $c \neq 0$，$\delta(c) \neq 0$

$\delta(c) = \delta(c \cdot 1) = \delta(c)\delta(1)$，两边相消得 $\delta(1) = 1$

$\therefore \delta(ab) = \delta(a)\delta(b) = \delta(1) = 1$

$\because \delta(a)$ 及 $\delta(b)$ 都是非负整数，$\therefore \delta(a) = 1$

若 $\delta(a) = 1$，则 $a \neq 0$，对于1及a，存在b，$\gamma \in A$，使得 $1 = ab + \gamma$，其中 $\delta(\gamma) < \delta(a) = 1$

$\because \delta(\gamma)$ 是 $\geqslant 0$ 的整数，$\therefore \delta(\gamma) = 0$，$\gamma = 0$

从而 $ab = 1$，即a是A的单位元。

4.令A是一个欧几里得整区，它的函数适合条件

$\delta(a + b) \leqslant \max[\delta(a), \delta(b)]$

验证：A或是一个域，或是域F上一个多项式整区F[x]

〔证〕：设A是欧几里得整区，令

$F = \{a \mid \delta(a) = 1, a \in A\} + \{0\}$

由第3题知，F的所有非零元都是A的单位元，因而F是A的子域。

若对A中的任意非零元b，都有$\delta(b)=1$，则$A=F$，此时A自身就是一个域。

若A中有非零元c，使得$\delta(c)>1$，则$A\supset F$。根据最小数原理，$A-F$中必存在一个元$x\neq 0$，使得对任意$c\in A-F$，都有
$$\delta(x)\leqslant\delta(c)$$

现证$A=F[x]$

$F[x]\subseteq A$是显然的。∵F中元当然包含在$F[x]$中，∴只要证对任意$a\in A-F$（此时$\delta(a)\geqslant 1$）都有$a\in F[x]$即可。由欧几里得整区的性质，存在q_1，$\gamma_1\in A$使得
$$a=q_1x+\gamma_1,\quad \delta(\gamma_1)<\delta(x)$$

∵$\delta(x)>1$，且$\delta(x)$在所有$\delta(a_i)>1$的$\delta(a_i)$中是最小的。

∴$\delta(\gamma_1)=0$或$\delta(\gamma_1)=1$，∴$\gamma_1\in F$，而且由$q_1x=a-\gamma_1$得
$$\delta(q_1)<\delta(q_1)\delta(x)=\delta(q_1x)=\delta(a-\gamma_1)\leqslant\max\{\delta(a),\ \delta(\gamma_1)\}=\delta(a)$$

即$\delta(q_1)<\delta(a)$

如果$\delta(q_1)\leqslant 1$，则$q_1\in F$，从而

$a=q_1x+\gamma_1\in F[x]$

如果$\delta(q_1)>1$，则重复上面步骤，存在$q_1,\gamma_1\in A$，使得
$$q_1=q_2x+\gamma_2,\quad \delta(\gamma_2)<\delta(x)$$

但因$\delta(a)$是有限的正整数，所以必有n，使得
$$\delta(a)>\delta(q_1)>\delta(q_2)>\cdots>\delta(q_n)=1$$

$\therefore q_n \in F$，而且

$$a=\gamma_1+\gamma_2 x+\cdots+\gamma_n x^{n-1}+q_n x^n \in F[x]$$

$\therefore A=F[x]$

再证x是关于F的超越元，即若$\sum_{i=0}^{n} a_i x^i=0$，必须$a_i=0$，$i=0, 1, \cdots, n$。这里$a_i \in F$。

假定$a_m \neq 0$，则$\delta(a_m)=1$，这里a_m是$a_0, a_1, \cdots, a_n$中最后一个不为0的系数，$-a_m x^m=\sum_{i=0}^{m-1} a_i x^i$

$$\delta(-a_m x^m)=\delta(a_m)\delta(x^m)=[\delta(x)]^m$$

而$\delta(\sum_{i=0}^{m-1} a_i x^i) \leqslant \max\{\delta(a_1 x), \cdots, \delta(a_{m-1} x^{m-1})\}$

$=\delta(a_k x^k)=[\delta(x)]^k$，这里$a_k$是$a_0, \cdots, a_{m-1}$中最后一个不为零的系数（$\because \delta(x)>1$）

因而得到$[\delta(x)]^m \leqslant [\delta(x)]^{m-1}$，这与$\delta(x)>1$的假设矛盾，因而所有的$a_i=0$

故$A=F[x]$是多项式整区。

习　题　50

1.如果$f(x) \in I[x]$，它的首项系数是1，并且它有一个有理根，求证：这个根是整数。

〔证〕：设$\frac{r}{s}$（r, s是互质的整数）是$f(x)$的一个有理根，

则$f(x)=(x-\frac{r}{s})g(x)$，$g(x)$是$R_0[x]$中$n-1$次多项式，（R_0是有理数域）

$$x-\frac{r}{s}=\frac{1}{s}(sx-r)，sx-r\text{为原多项式}$$

$$g(x)=\frac{m}{n}g_1(x)，g_1(x)\text{为原多项式}$$

$$\therefore f(x)=\frac{m}{sn}(sx-r)g_1(x)\overset{令}{=}\frac{p}{q}(sx-r)g_1(x)，$$

$(p,q)=1$

$\because f(x)$是整系数多项式，$\therefore (sx-r)g_1(x)$各项系数与p的乘积必须被q所整除，但因$(p,q)=1$，所以q必须整除$(sx-r)g_1(x)$的所有系数，又$\because (sx-r)g_1(x)$是原多项式$\therefore q=1$。

$\therefore f(x)=p(sx-r)g_1(x)=(sx-r)\cdot pg_1(x)=(sx-r)f_1(x)$，$f_1(x)$的首项系数也是1。比较两边系数即知$s=1$

$\therefore \frac{r}{s}=r$，即$f(x)$的有理根是整数。

2.求证下面的爱森斯坦(Eisenstein)不可约性判别准则：如果$f(x)=a_0+a_1x+\cdots+a_nx^n\in I[x]$，并且存在有素数$p\in I$使$p\mid a_0$，$p\mid a_1$，…，$p\mid a_{n-1}$，但$p\nmid a_n$（$p$不是$a_n$的因子），而且$p^2\nmid a_0$，则$f(x)$在$I[x]$里不可约，从而在$R_0[x]$里也是不可约，这里$R_0$是有理数域。

〔证〕：若$f(x)=a_0+a_1x+\cdots+a_nx^n$在$I[x]$里可约，即

$$f(x)=\left(\sum_{i=0}^{l}b_ix^i\right)\left(\sum_{j=0}^{m}c_jx^j\right)，(l,m<n\text{且}l+m=n，$$

c_j，$b_i\in I$，比较两边系数有

$$a_n=b_lc_m，a_0=b_0c_0$$

因为$p\mid a_0$，而p是素数，∴ 必有$p\mid b_0$或$p\mid c_0$，但，∵$p^2\nmid a_0$∴不能有$p\mid b_0$且$p\mid c_0$，不妨假定$p\mid b_0$但$p\nmid c_0$另一方面，因为$p\nmid a_n$，所以$p\nmid b_l$

设b_0，b_1，…，b_l中第一个不能被p整除的是b_k

∵$a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k$

式中a_k，b_{k-1}，…，b_0都能被p整除，所以b_kc_0也必能被p整除，因为p是素数，所以b_k与c_0中至少有一个可被p整除，这就得出矛盾。所以f(x)在I[x]中不可约。根据引理3，f(x)在R_0[x]中也不可约。

3.如果p是一个素数，验证：以x+1代替

$$x^{p-1}+x^{p-2}+\cdots+1=(x^p-1)/(x-1)$$

里的x所得的多项式在R_0[x]里是不可约的，由此证明割园多项式$x^{p-1}+x^{p-2}+\cdots+1$在R_0[x]里是不可约的。

〔证〕：设$f(x)=x^{p-1}+x^{p-2}+\cdots+1=(x^p-1)/(x-1)$

$$f(x+1)=(x+1)^{p-1}+(x+1)^{p-2}+\cdots+1=$$

$$(x+1)^p-1/x=x^{p-1}+c^1{}_px^{p-2}+\cdots+c_p{}^{p-1}$$

∵p是素数，由习题47第3题知$p\mid c^i{}_p$，$i=1$，…，$p-1$，且$p^2\nmid c_p{}^{p-1}=p$，$p\nmid 1$，∴由上题Eisenstein不可约性判别准则知$f(x+1)=x^{p-1}+c^1{}_px^{p-2}+\cdots+p$在$R_0$[x]中不可约。由此即得割园多项式$f(x)=x^{p-1}+x^{p-2}+\cdots+1$在$R_0$[x]中也不可约。因为如果f(x)在$R_0$[x]中可约，即

$$f(x)=x^{p-1}+x^{p-2}+\cdots+1=f_1(x)f_2(x)$$

$$0<\deg f_1(x),\ \deg f_2(x)<p-1$$

于是$f(x+1)=x^{p-1}+c^1{}_px^{p-2}+\cdots+p$

$$=f_1(x+1)f_2(x+1)$$

$$\deg f_1(x+1)=\deg f_1(x),\ \deg f_2(x+1)=$$

$\deg f_2(x)$

因而得到f(x+1)也可约的错误结论。

第五章　带算子群

习　题　51

1. 求证：G的特征（全不变）子群H的任一个特征（全不变）子群K是G的特征（全不变）子群。

证：设$\overline{m}$是G的任一自同构，由H是G的特征子群，有$H\overline{m}\subseteq H$。因而$\overline{m}$限制在子群H上，得出H上的一个自同构，记为$\overline{m}H$，即$H\overline{m}=H\overline{m}_H$。即$Hm=H\overline{m}_H$，由K是H的特征子群，所以有$K\overline{m}_H\subseteq K$。

于是得$K\overline{m}\subseteq K$，又K是H的子群，H是G的子群，所以K是G的子群，故K是G的特征子群。

同理，设$\overline{m}$是G的任一自同态，有$H\overline{m}\subseteq H$，记$\overline{m}H$；$H\overline{m}=H\overline{m}_H\subseteq H$，于是有$K\overline{m}=K\overline{m}_H\subseteq K$，即K是G的全不变子群。

2. 求证：循环群的任一个子群是全不变的。

证：设所给循环群为〔a〕，它的全部自同态的集合为M。

则任意$\overline{m}\in M$，有$a\overline{m}=a^{n_m}$，（其中n_m是正整数或0）

〔由$a^r\overline{m}=(a\overline{m})^r=(a^{n_m})^r$〕

而循环群〔a〕的任一子群可表为〔a^s〕，s是正整数。

则由$a^s\overline{m}=(a\overline{m})^s=(a^{n_m})^s=(a^s)^m\in$〔$a^s$〕

知〔a^s〕对〔a〕的所有自同态映照都把它映到自身内，所以〔a^s〕是全不变子群。

3. 求证：由所有换位子$[s,t]=sts^{-1}t^{-1}$生成的子群$G^{(1)}$是一个全不变子群，这里$s,t\in G$，$G^{(1)}$叫做G的（第一）换位子群，证明：$G/G^{(1)}$是交换群，并且如果H是任一个不变子群能使G/H是交换群时，则$G^{(1)}\subseteq H$。

证：设$\overline{m}$是G的任意自同态，则有$s\overline{m}\in G$，$t\overline{m}\in G$。

又$s^{-1}\overline{m}=(s\overline{m})^{-1}$，$t^{-1}\overline{m}=(t\overline{m})^{-1}$

于是$(sts^{-1}t^{-1})\overline{m}=(s\overline{m})(t\overline{m})(s\overline{m})^{-1}(t\overline{m})^{-1}\in G^{(1)}$

即G中任意换位子经G的任一自同态$\overline{m}$映照后，仍是G的换位子。

故$G^{(1)}$是G的全不变子群。

其次，证明$G/G^{(1)}$是交换群。

对任意$x,y\in G$，则$x^{-1}y^{-1}xy=g\in G^{(1)}$

于是有$xy=yxg$，$\Rightarrow xyG^{(1)}\subseteq yxG^{(1)}$

同理有$y^{-1}x^{-1}yx=g_1\in G^{(1)}$，得$yx=xyg_1\Rightarrow$
$yxG^{(1)}\subseteq xyG^{(1)}$

$\therefore xyG^{(1)}=yxG^{(1)}$，即$(xG^{(1)})(yG^{(1)})=xyG^{(1)}$
$yxG^{(1)}=(yG^{(1)})(xG^{(1)})$

所以$G/G^{(1)}$是交换群。

第三，若G/H是交换群。

即对任意$x,y\in G$，有$(xH)(yH)=(yH)(xH)$

即$xyH=yxH$，$\rightarrow xy\in yxH$

$\therefore \exists h\in H$，$xy=yxh$，得$h=x^{-1}y^{-1}xy$

即任一换位子都包含在H中，而$G^{(1)}$中元是有限个换位子的积，又H是G的子群，所以得由换位子生成的子群$G^{(1)}\subseteq H$。

4. 令A是带恒等元素环，并取$M=A_r$，而把A看作一个

一群。问A的M—自同态是什么？如果取$M=A_r\cup A_l$，则A的M—自同态是什么？

解：（1）$\because M=A_r$，设η是A的任一M—自同态，则对，$\forall x\ y\in A$

有$(x+y)\eta=x\eta+y\eta$，$(xy)\eta=(x\eta)y$

又恒等元$1\in A$，则对A中任意元x有

$x\eta=(1\cdot x)\eta=(1\cdot\eta)x$，$1\eta\in A$

即任一M—自同态η作用于A中任意元x，相当于用A中元1η左乘于x。反之，A_l（即A中左乘变换全体）中元显然是M—自同态，$\because\forall a\in A$，$a_l\in A_l$：

$a_l(x+y)=a(x+y)=ax+ay=a_lx+a_ly$

$a_l(xy)=a(xy)=(ax)y=(a_lx)y$

则A的M—自同态是A_l。

（2）$M=A_r\cup A_l$

则任一M—自同态η：$\forall x,\ y\in A$

$(x+y)\eta=x\eta+y\eta$，$(xy)\eta=(x\eta)y=x(y\eta)$

$\because 1\in A$，$\therefore x\eta=(1\cdot x)\eta=(1\cdot\eta)x=x(1\cdot\eta)$，对$x\in A$。

即$1\eta\in A$的中心C，显然用C中元右乘A中元x与去左乘A中元x是一样的。记C_r为用C中元去右乘A中元所得的右乘变换的集合。于是任一M—自同态η，相当于用C中元(1η)所得的右乘变换。反之，C_r中任一元，都是A的一个M—自同态。$\because c\in C$，$c_r\in C_r$，$c_r(x+y)=c(x+y)=cx+cy=c_rx+c_ry$

$c_r(xy)=c(xy)=(cx)y=(c_rx)y$

又$c_r(xy)=(xy)c=x(yc)=x(cy)=x(c_ry)$

则A的M—自同态是c_r全体。

习　　题　　52

1.决定$I/(m)$（$m>0$）的理想。

解：$I/(m)$（$m>0$）的所有理想，由I中包含（m）的所有理想所完全决定，而I中包含（m）的任一理想$(n)\sqsupseteq(m)\Leftarrow\Rightarrow n\mid m$，（∵I是主理想整区）故$I/(m)$的全部理想的集合是$\{(n)/(m)\mid n|m\}$。

2.试直接导出一个环的理想与这个环的一个同态象的理想之间的对应。

证：设A′是环A的一个同态象，即存在一个由A到A′上的同态映照η，使$A\eta=A'$，则

1）$\eta^{-1}(0')=K$，显然是A的一个理想。且$A'\cong A/K$

2）设B是A中任一包含K的理想，则$B\eta$是A′的理想。

∵对b_1'，$b_2'\in B\eta$，则在存b_1，$b_2\in B$，使$b_1\eta=b_1'$
$b_2\eta=b_2'$

∴$b_1'-b_2'=b_1\eta-b_2\eta=(b_1-b_2)\eta\in B\eta$

又对$a'\in A'$，则存在$a\in A_S$，$a\eta=a'$

于是$a'b_1'=(a\eta)(b_1\eta)=(ab_1)\eta\in B\eta$

$b_1'a'=(b_1\eta)(a\eta)=(b_1a)\eta\in B\eta$

3）B_1，B_2都是A中包含K的理想，若$B_1\eta=B_2\eta$，则$B_1=B_2$，先证$\eta^{-1}(B_1\eta)=B_1$

设$\eta^{-1}(B_1\eta)=C_1$，显然$C_1\sqsupseteq B_1$

又对c_1C_1，则存在$b_1\in B_{1S}$，$c_1\eta=c_1\eta$

$\rightarrow c_1=b_1+k_1$，$k_1\in K$，∵$B_1\sqsupseteq K$，∴$b_1+k_1\in B_1$，得$C_1\sqsubseteq B_1$，故$C_1=B_1$

再证：若$B_1\eta = B_2\eta$，则$B_1 = B_2$

$\because B_1 = \eta^{-1}(B_1\eta) = \eta^{-1}(B_2\eta) = B_2$

4）设B'是A'的任一理想，则$B = \eta^{-1}(B')$是A的理想，且$K\subseteq B$。

$\because \forall b_1, b_2 \in B$，即$b_1\eta, b_2\eta \in B'$

$\therefore$ 由$(b_1 - b_2)\eta = b_1\eta - b_2\eta \in B'$得$b_1 - b_2 \in B$

又$\forall a \in A$，有$(ab_1)\eta = (a\eta)(b_1\eta) \in B'$

$(b_1 a)\eta = (b_1\eta)(a\eta) \in B'$

即$ab_1 \in B$，$b_1 a \in B$，故B是A的理想。

显然$B \supseteq K$，$\because 0' \in B'$，$\therefore \eta^{-1}(0') \subseteq B$，即$K \subseteq B$

这就建立了A里包含K的各理想的集合$\{B\}$与A'里理想的全体之间的一个1－1对应。

习　题　53

1.求证：从第三同构定理可推得第二同构定理。

证：第三同构定理是：G'_i及G_i（$i = 1, 2$）是G的M—子群，而G'_i是G_i的不变子群，则$(G_1 \cap G'_2)G'_1$是$(G_1 \cap G_2)G'_1$的不变子群，$(G'_1 \cap G_2)G'_2$是$(G_1 \cap G_2)G'_2$的不变子群，并且它们的对应商群是M—同构的。

我们取$G_1 = H_1$是G的任一M—子群，$G_2 = G$

$G'_1 = \{1\}$，1是G的恒等元。$G'_2 = H_2$是G的任一不变M—子群，于是第三同构定理的条件都满足，通过计算得：

$(G_1 \cap G_2)G'_2 = (H_1 \cap G)H_2 = H_1 H_2$

$(G'_1 \cap G_2)G_2' = (\{1\} \cap G)H_2 = 1 \cdot H_2 = H_2$

$(G_1 \cap G_2)G'_1 = (H_1 \cap G)\{1\} = H_1 \cdot 1 = H_1$

$(G_1 \cap G'_2)G'_1 = (H_1 \cap H_2)\{1\} = H_1 \cap H_2$

依据第三同构定理得

$H_1H_2/H_2 \cong H_1/H_1 \cap H_2$，此即第二同构定理。

2.令G_1，G'_1是M—子群，而G'_1是G_1的一个不变子群，并令H是G的任一个M—子群，求证：$H'_1 = G'_1 \cap H$，是$H_1 = G_1 \cap H$的不变子群，并且H_1/H'_1同构于G_1/G'_1的一个子群。

证：（1）先证H'_1是H_1的不变子群

$\forall x \in H_1$，$\forall y \in H'_1$，则$x \in H$，$y \in H$，$\therefore x^{-1}yx \in H$

又$x \in G$，$y \in G'_1$，而G'_1是G_1的不变子群，$\therefore x^{-1}yx \in G'_1$

故$x^{-1}yx \in G'_1 \cap H = H'_1$

（2）由$H_1/H'_1 = G_1 \cap H/G'_1 \cap H = G_1 \cap H/(G'_1 \cap H) \cap G^1 = G_1 \cap H/(G_1 \cap H) \cap G'_1$

$$= H_1/H_1 \cap G'_1 \cong H_1G'_1/G'_1$$

（这里依据第二同构定理）

显然$H_1G'_1 = (G_1 \cap H)G'_1$是$G_1$的子群。且$(G_1 \cap H)G'_1 \supseteq G'_1$。

又满足$(G_1 \cap H)G'_1 \cdot G'_1 = G'_1 = (G_1 \cap H)G'_1$

（$\because G'_1$是G_1的不变子群）所以H_1G_1'/G_1'是G_1/G_1'的一个子群。

3.说出关于环上类似的第一及第二同构定理。

解：第一同构定理：设η是环A到环A′上的一个同态，K是同态核。并设B是A里包含着K的一个理想，则$B^\eta = B'$是A′的理想，並且差环A/B与A′/B′在对应$a + B \to a^\eta + B'$下是同构的。

第二同构定理：如果A_1及A_2是一个环A的子环，并且A_2是理想，则（1）$A_1 \cap A_2$是A_1的理想，并且（2）差环$A_1 + A_2/A_2$与$A_1/A_1 \cap A_2$在对应$a_1 + A_2 \to a_1 + (A_1 \cap A_2)$下是同构的。

习　题　54

1.如果$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{s+1} = 1$是G的一个正规群列，并且H是任一个M—子群，求证：

$$H = (H \cap G_1) \supseteq (H \cap G_2) \supseteq \cdots \supseteq (H \cap G_{s+1}) = 1$$

是H的一个正规群列，并求证后者各个商同构于前者各个商的子群。

证：显然本题是习题53第2题的直接推论，

即$H \cap G_{i+1}$是$H \cap G_i$的不变子群（$i = 1, 2, \cdots, s$）

且$(H \cap G_i)/(H \cap G_{i+1}) \cong (H \cap G_i)G_{i+1}/G_{i+1}$；

$(H \cap G_i)G_{i+1}/G_{i+1}$是$G_i/G_{i+1}$的子群。

2.如果一个普通群有一个正规群列，它的各个商都是交换群时，则这个普通群叫做可解群。证明：一个可解群的任一个子群及任一个商群都是可解的。

证：设G为可解群，则G有一个正规群列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{s+1} = 1$$

且每个商群G_i/G_{i+1}是可换群（$i = 1, 2 \cdots s$）

（1）设H为G的任一子群，依第1题知

$$H = (H \cap G_1) \supseteq (H \cap G_2) \supseteq \cdots \supseteq (H \cap G_{s+1}) = 1$$

是H的一个正规群列，并且每一个商群$(H \cap G_i)/(H \cap G_{i+1})$与$G_i/G_{i+1}$的子群同构，所以也是可换群，于是H也是可解群。

（2）设H是G的任一商群，依群的同态基本定理知，H是G的一个同态象，记此同态为η，即$H=G\eta$。

今证$H=G\eta=G_1\eta\supseteq G_2\eta\supseteq\cdots\supseteq G_{s+1}\eta=1$是H的正规群列，且$G_i\eta/G_{i+1}\eta$（$i=1,2\cdots s$）是可换群，则H是可解群，显然$G_i\eta$是$G\eta$的子群。先证$G_{i+1}\eta$是$G_i\eta$的不变子群。

$\forall g\in G_{i+1}\eta$，则存在$g'\in G_{i+1}$使$g'\eta=g$

$\forall x\in G_i\eta$，则存在$x'\in G_i$，使$x'\eta=x$

于是$x^{-1}gx=(x'\eta)^{-1}(g'\eta)(x'\eta)=(x'^{-1}g'x')\eta$

由G_{i+1}是G_i的不变子群，$\therefore x'^{-1}g'x'\in G_{i+1}$，得$x^{-1}gx\in G_{i+1}\eta$，其次证$G_i\eta/G_{i+1}\eta$是可换群.

由G_i/G_{i+1}是可换群，即$\forall h, g\in G_i$

$$(hG_{i+1})(gG_{i+1})=(gG_{i+1})(hG_{i+1})$$

显然上述关系在同态映照下不变，即

$$[(h\eta)G_{i+1}\eta][(g\eta)G_{i+1}\eta]=[(g\eta)G_{i+1}\eta][(h\eta)G_{i+1}\eta]$$

故得H是可解群

3．设归纳地定义G的高阶导群$G^{(i)}=(G^{(i-1)})^{(1)}$（参看习题51第3题）

求证G是可解群，必须且只须有整数s存在，使$G^{(s)}=1$

证：（充分性）因为此时有

$G=G^{(0)}\supseteq G^{(1)}\supseteq G^{(2)}\supseteq\cdots\supseteq G^{(s)}=1$

由习题51第3题知$G^{(i+1)}$是$G^{(i)}$的正规子群，且$G^{(i)}/G^{(i+1)}$是可换群，所以G是可解群。

（必要性）已知G是可解群。故有正规群列

$$G=G_1\supseteq G_2\supseteq\cdots\supseteq G_{s+1}=1$$

且每个G_i/G_{i+1}是可换群（$i=1,2,\cdots s$）.

由G_1/G_2是可换群，知$G_1^{(1)}\subseteq G_2$，又由G_2/G_3是可换群

$\therefore G_2^{(1)}\subseteq G_3$，$\because G^{(2)}=G_1^{(2)}\subseteq G_2^{(1)}\subseteq G_3$，利用归纳法可证得$G^{(i)}\subseteq G_{i+1}$（$i=1,2,\cdots s$）

于是有整数s，使$G^{(s)}\subseteq G_{s+1}=1$，即$G^{(s)}=1$。

4.求证：阶数是素数幂的任一有限群必为可解群（参看习题20第3题）

证：假定群G的阶数是p^n，p为素数，对n施行归纳法来证明

（1）$n=1$时，G是循环群，因而是可换群，故G是可解群。

（2）归纳假设$1\leqslant k<n$时命题成立，今证阶为p^n时也成立。由习题20第3题知，G的中心C的元数大于1，于是$\bar{G}=G/C$的元数是p^k，$k<n$，依归纳假设，$\bar{G}$是可解群，即存在整数s使$\bar{G}^{(s)}=1$。另一方面$\bar{G}$是G的同态象，且$\bar{G}^{(k)}$的象是$G^{(k)}$。因此有$G^{(s)}\subseteq C$，C是可换群，所以是可解群，于是存在整数t使$C^{(t)}=1$，则$G^{(s+t)}\subseteq C^{(t)}=1$

即$G^{(s+t)}=1$，故G是可解群。

习　　题　　55

1.应用约当—霍尔德定理于有限循环群，以证明一个正整数分解为正素数因子的唯一性。

〔证法一〕设n为任一正整数，构造一个阶为n的循环群记为$[a]=G$。

则G适合链条件，故有合成群列。

命$G=G_1\supset G_2\supset G_3\supset\cdots\supset G_{s+1}=1$

是G的一个合成群列，其中G_i/G_{i+1}是素数阶的循环群。阶数用p_i表示（$i=1,2\cdots,s$）

则$n=p_1p_2\cdots p_s$，p_i是素数。

由约当—霍尔德定理知：G的任意两个合成群列是等价。即其商群列存在相互同构的一一对应，而同构的循环群具有相同的阶数，这就证明了n的素数因子由n唯一决定。

〔证法二〕设〔a〕是n阶循环群，n分解成正素数的两种分解式为$n=p_1p_2\cdots p_s=p'_1p'_2\cdots p'_t$ 显然$[a]\supset[a^{p_1}]\supset[a^{p_1p_2}]\supset\cdots\supset[a^{p_1p_2\cdots p_s}]=1$，$[a]\supset[a^{p'_1}]\supset[a^{p'_1p'_2}]\supset\cdots\supset[a^{p'_1p'_2\cdots p'_t}]=1$是〔a〕的两个合成群列。由约当—霍尔德定理知，这两个合成群列是等价的，故它们的商群之间构成1－1对应，且对应的商群是同构的，又同构的有限群有相同的阶数，令两商群列的阶数分别为p_1，p_2，…，p_s和p'_1，p'_2，…，p'_t，故p_i必与等p'_i相等，经过次序适当调整后，有$p_i=p'_i$（$i=1,2,\cdots,s$）且$s=t$。这就证明了n的分解式除次序外是唯一的。

2.如果G有一个合成群列，求证：如果G的任一个正规群列里各项是真递减的，则可加细为一个合成群列。

证：设$G=G_1\supset G_2\supset G_3\supset\cdots\supset G_t=1$ ………（1）

是G的正规群列，且各项是真递减的

又$G=H_1\supset H_2\supset\cdots\supset H_{s+1}=1$，是G的合成群列

因为合成群列也是正规群列，依叔莱尔加细定理知，这两个正规群列有等价的加细。而合成群列的加细，最多只能添加一些原有的项。而相邻两项相同的商群的阶是1，在（1）的等价加细中，去掉与合成群列加细后出现的重复项，相应的项后，得到的仍是一对等价的正规群列，此时（1）这

样加细后的正规群列就是一个合成群列。

3.如果G有一个合成群列，求证：G的任一个不变子群及G的任一个商群各有合成群列；并求证：这些群列的合成商是M—同构于G的合成商。

〔证一〕设H是G的任一不变子群；G/K是G的任一商群，即K是G的一个不变子群。于是$G\supset H\supseteq 1$及$G\supset K\supseteq 1$，是G的两个正规群列，且可设其为真递减的，若$H=G$（或$H=1$）正规群列为$G\supset 1$，同样地若$K=G$（或$K=1$）同样处理。

由第2题，它们分别可加细成为一个合成群列。当然这些合成群列与G的任一合成群列是等价的，于是合成商是互相M—同构的。

〔证二〕1）设H是G的任一不变子群，若$H=G$或$H=1$则H自然有一合成群列，不妨设$G\supset H\supset 1$，∵$G\supset H\supset 1$是G的一个正规群列，由题2知可加细为G的一个合成群列，设为

$$G=G_1\supset G_2\supset\cdots\supset G_s\supset H=H_1\supset H_2\supset\cdots\supset H_{t+1}=1$$

显然$H=H_1\supset H_2\supset\cdots\supset H_t\supset H_{t+1}=1$是H的一个合成群列，此时，它的各个商自然同构于G的合成商。

2）对G的正规子群H取第一步中的$G_1, G_2, \cdots, G_s$，考察$G/H=G_1/H\supset\cdots\supset G_s/H\supset H/H=1$

因H是G的不变子群，当然也是G_i（$i=1, 2, \cdots, s$）的不变子群，由第一同构定理知

$$G_i/H/G_{i+1}/H\cong G_i/G_{i+1}$$

∵G_i/G_{i+1}是M—单纯群，故$G_i/H/G_{i+1}/H$也是M—单纯群

$\therefore G/H=G_1/H\supset G_2/H\supset\cdots\supset G_s/H\supset H/H=1$
是G/H的一个合成群列，且合成商同构于G的合成商。

习　题　56

1.求S_3及S_4的合成群列。

解：$S_3\supseteq A_3\supseteq 1$是$S_3$的正规群列

又它们的商群列S_3/A_3，A_3的阶数是2，3都是素数，故都是单纯群，于是$S_3\supset A_3\supset 1$是S_3的合成群列。

令$B_4=\{(1),(12)(34),(13)(24),(14)(23)\}$

$C_4=\{(1),(12)(34)\}$

则$S_4\supset A_4\supset B_4\supset C_4\supset 1$是$S_4$的正规群列

且它们的商群列S_4/A_4，A_4/B_4，B_4/C_4，C_4的阶数分别为2，3，2，3都是素数，故都是单纯群，所以上述正规群列也是S_4的合成群列。

2.求证：一个有限群是可解的必须而且只须它的合成商都是素数阶的循环群。

证：必要性：设G是有限群，又是可解群，于是G有正规群列，且它的各个商都是交换群。另一方面，有限群适合升链及降链条件，故G有合成群列，而每个正规群列都可加细为合成群列，这时G的合成群列的各个商都是有限，可换，单纯群。一个有限、可换、单纯群一定是素数阶的循环群。

充分性：设G有合成群列，且其合成商都是素数阶的循环群，当然是可交换群，依定义，这个合成群列，即所要求的正规群列，因而G可解。

必要性的第二种证法：

设有限群G是可解群，$G=G_1\supset G_2\supset\cdots\supset G_{s+1}=1$是商群列都是交换群的一个正规群列，因有限群必有合成群列，由题2知它可加细为合成群列，设为$G=H_1\supset H_2\supset\cdots\supset H_{l+1}=1$。又设$G_i=H_t\supset H_{t+1}\supset\cdots\supset H_{t+k}=G_{i+1}$。因$G_{i+1}$是$G_i$的正规子群，当然$G_{i+1}$也是$H_{t+j}$（$j=0,1,2,\cdots,k$）的正规子群，由第一同构定理知

$$H_{t+j}/H_{t+j+1}\cong H_{t+j}/G_{i+1}/H_{t+j+1}/G_{i+1}$$
$$(j=0,1,2,\cdots,k)$$

因G_i/G_{i+1}可交换，故H_{t+j}/G_{i+1}可交换，于是

$H_{t+j}/G_{i+1}/H_{t+j+1}/G_{i+1}$可交换，所以$H_{t+j}/H_{t+j+1}$可交换，$H_j/H_{j+1}$（$j=1,2,\cdots,l$）可交换。

由$G=H_1\supset H_2\supset\cdots\supset H_{l+1}=1$是合成群列，知对应的各商群$H_j/H_{j+1}$是M—单纯群，且由G是有限群，知$H_j/H_{j+1}$也是有限群，因而是素数阶循环群。

3.求证：一个无限循环群（$M=\phi$）适合升链条件，但不适合降链条件。

证：设$G=(a)$是一个无限循环群，则G的任一子群也是循环群，且可表为(a^s)，其中s是整数。

显然$(a^s)\sqsubseteq(a^t)$的充要条件是$t\mid s$。（t是s的因子）今证G适合升链条件，设G的任一子群列。

$$(a^{m_1})\sqsubseteq(a^{m_2})\sqsubseteq(a^{m_3})\sqsubseteq\cdots$$

因为m_1是整数，且$m_2\mid m_1,\cdots,m_{i+1}\mid m_i$（$i=1,2,\cdots$）而$m_1$的正因数的个数只有有限个，故必定存在有正整数n，使得$m_{n+1}=m_{n+2}=\cdots$

即$(a^{m_{n+1}})=(a^{m_{n+2}})=\cdots$

其次，G不适合降链条件，因

$$[a]\supset[a^2]\supset[a^4]\supset[a^8]\supset\cdots$$

显然是一个无限递降子群列。

4．令U(p)是1的p^k个复根的乘法群，这里p是固定的素数，而k＝0，1，2，3，…求证：U(p)的各个真子群是有限循环群。于是，求证：U(p)适合降链条件，但不适合升链条件。

证：∵ $U(p)=\left\{e^{\frac{2l_k\pi i}{p^k}}\middle|k=0,1,2,\cdots;l_k=0,1,2,\cdots,p^{k-1}\right\}$ 是一个无限可交换群。设H是U(p)的任一真子群，则存在某个最小正整数q，使得$e^{\frac{2l\pi i}{p^q}}\in U(p)$ $e^{\frac{2l\pi i}{p^q}}\notin H$，且$(l,p)=1$。于是对任意整数$r\geq q$，有$e^{\frac{2l\pi i}{p^r}}\notin H$，否则，若$e^{\frac{2l\pi i}{p^r}}\in H$，则$\left[e^{\frac{2l\pi i}{p^r}}\right]=\left[e^{\frac{2\pi i}{p^r}}\right]\subseteq H$于是$e^{\frac{2p^{r-q}\pi i}{p^r}}=e^{\frac{2\pi i}{p^q}}\in H$，与原设矛盾。

$\therefore H\subseteq\left[e^{\frac{2\pi i}{p^{q-1}}}\right]$，又$e^{\frac{2\pi i}{p^{q-1}}}\in H$

得$H=\left[e^{\frac{2\pi i}{p^{q-1}}}\right]$即H是$p^{q-1}$阶循环群

其次：

$$(1)\subset\left[e^{\frac{2\pi i}{p}}\right]\subset\left[e^{\frac{2\pi i}{p^2}}\right]\subset\cdots\subset\left[e^{\frac{2\pi i}{p^n}}\right]\subset\cdots$$

是U(p)的一个无限递升的不变M—子群列。故知U(p)不适合升链条件。

但U(p)却适合降链条件。否则，U(p)若有一个无限真递降子群列

$$U(p)\supset H_1\supset H_2\supset\cdots\supset H_s\supset\cdots$$

其中H_i都是有限循环群。用$[H_i:H_{i+1}]$表H_i/H_{i+1}的阶。则有$[H_1:1]=[H_1:H_2][H_2:H_3]\cdots[H_i:H_{i+1}]\cdots$，此不可能，因为左边是一有限整数，而右边却是无限个大于1的整数的乘积，故$U(p)$适合降链条件。

习　　题　　57

1.从直接证明下面的结果来证明定理6：如果b是$n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$阶的一个元素，则$b=b_1b_2\cdots b_s$，这里$b_i$的阶数为$p_i^{e_i}$。

证：令$q_i=\dfrac{n}{p_i^{e_i}}$ $(i=1, 2,\cdots,s)$，$\because i\neq j, p_i\neq p_j$，且$p_i$是素数，$\therefore q_1, q_2, \cdots, q_s$的最大公因数$=1$，于是存在整数$\lambda_1, \lambda_2, \cdots, \lambda_s$，使得$\lambda_1q_1+\lambda_2q_2+\cdots+\lambda_sq_s=1(*)$，则$b=b^{\lambda_1q_1+\cdots+\lambda_sq_s}=b^{\lambda_1q_1}b^{\lambda_2q_2}\cdots b^{\lambda_sq_s}$ 记$b^{\lambda_iq_i}=b_i$ $(i=1, 2\cdots, s)$即$b=b_1b_2\cdots b_s$，今证b_i的的阶数是$p_i^{e_i}$

由$b_i^{p_i^{e_i}}=(b^{\lambda_iq_i})^{p_i^{e_i}}=b^{\lambda_in}=(b^n)^{\lambda_i}=1$

从（*）式可看出λ_i不可能有p_i的因数，$\because$当$j\neq i$时，q_j含有因数$p_i^{e_i}$，若λ_i再含有因数p_i，则（*）式右边至少是$p_i\neq 1$，此不可能。于是得b_i的阶数是$p_i^{e_i}$。

今利用它证明定理6。

定理6．如果G是$n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$阶有限循环群，这里$p_i$是素数，并且$i\neq j$时，$p_i\neq p_j$，则$G$是$p_i^{e_i}$ $(i=1, 2, \cdots, s)$阶的循环群的直接积。

证：令G_i是G中阶为$p_i^{e_i}$的元素连同1所成的子群，显然G_i是$p_i^{e_i}$阶循环群。

对$\forall g\in G$，则g是n阶元素，故$g=g_1g_2\cdots g_s$，其中g_i是$p_i^{e_i}$阶元素，$\therefore g_i\in G_i$，于是$G=G_1G_2\cdots G_s$

再证$G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_s=1$（$i=1,2,\cdots s$）

设$\forall z\in G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_s$，即z是$p_i^{e_i}$阶元素，同时又是$q_i=\dfrac{n}{p_i^{e_i}}$阶元素。而$(p_i^{e_i}, q_i)=1$，$\therefore$存在整数$\lambda,\mu$，使$\lambda p_i^{e_i}+\mu q_i=1$，则$z=z^{\lambda p_i^{e_i}+\mu q_i}$

$=(z^{p_i^{e_i}})^{\lambda}(z^{q_i})^{\mu}=1\cdot 1=1$ 于是$G=G_1\times G_2\times\cdots\times G_s$。

2.如果G是$n=st$阶循环群，这里$(s,t)=1$。求证：$G=H\times R$，这里H的阶数是s，而R的阶数是t。

证：设$G=[a]$，a的阶数是n。由$(s,t)=1$，故存在整数u，v，使$ut+vs=1$，于是$a=a^{ut+vs}=(a^t)^u\cdot(a^s)^v$

令$H=[a^t]$，$R=[a^s]$，则H，R分别为s,t阶循环群。

故(1)$G=HR$

$\forall b\in H\cap R$，则$b\in[a^t]$，$\therefore b=a^{th}$

又$b\in[a^s]$，$\therefore b=a^{sk}$，即$a^{th}=a^{sk}$，于是$th\equiv sk(\mathrm{mod}\, n)$

即$th-sk=mn=mst$，于是$th=s(mt+k)$由$(s,t)=1$，

得$s\mid h$，记$h=sh_1$，于是$b=a^{th}=a^{tsh_1}=a^{nh_1}=1$故

(2)$H\cap R=1$

所以$G=H\times R$

3.如果G是$n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$阶有限交换群，这里$p_i$

是不同的素数。

求证：$G=G_1\times G_2\times\cdots\times G_s$，这里$G_i$是一个子群，它的所有元素的阶数是$p_i$的幂。

证：令$G_i=\{x \mid x\in G: x^{p_i^{e_i}}=1\}$

$(i=1, 2, \cdots, s)$

则G_i是G的子群，∴$a, b\in G_i$，即$a^{p_i^{e_i}}=1$，$b^{p_i^{e_i}}=1$

于是有$(ab)^{p_i^{e_i}}=1$，$(a^{-1})^{p_i^{e_i}}=(a^{p_i^{e_i}})^{-1}=1^{-1}=1$，∴$ab\in G_i$，$a^{-1}\in G_i$

其次证$G=G_1\times G_2\times\cdots\times G_s$

（1）由于G是交换群，故G_i中任意元与G_j中任意元可交换。

（2）G中每一元有且仅有一种方 法表成$g_1g_2\cdots g_s$，$g_i\in G_i$。

∵p_i是不同的素数，令$q_i=\dfrac{n}{p_i^{e_i}}$（$i=1, 2, \cdots, s$）

则$q_1, q_2, \cdots, q_s$的最大公因数是1，因此有整数λ_1，$\lambda_2, \cdots, \lambda_s$存在，使$\lambda_1q_1+\lambda_2q_2+\cdots+\lambda_sq_s=1$

对$\forall g\in G$，$g=g^{\lambda_1q_1+\cdots+\lambda_sq_s}=g^{\lambda_1q_1}g^{\lambda_2q_2}\cdots g^{\lambda_sq_s}$

但$(g^{\lambda_iq_i})^{p_i^{e_i}}=g^{\lambda_in}=(g^n)^{\lambda_i}=1$，∴$g^{\lambda_iq_i}\in G_i$（$i=1, 2, \cdots, s$）

即G中任一元$g=g_1g_2\cdots g_s$，$g_i\in G_i$，其中$g_i=g^{\lambda_ig_i}$

再证表法唯一，若$g_1g_2\cdots g_s=1$，$g_i\in G_i$

$\because g_i^{p_i^{e_i}}=1$，$\therefore g_i^{q_j}=1$（$i\neq j$）

于是$g_1^{q_1}g_2^{q_2}\cdots g_i^{q_i}\cdots g_s^{q_s}=1^{q_i}=1$，即$g_i^{q_i}=1$

但（q_i，$p_i^{e_i}$）$=1$，故有整数u，v存在，使$uq_i+vp_i^{e_i}=1$

于是$g_i=g_i^{uq_i}\cdot g_i^{vp_i^{e_i}}=(g_i^{q_i})^u(g_i^{p_i^{e_i}})^v=1\cdot 1=1$（$i=1,2,\cdots,s$）

依定理7，$G=G_1\times G_2\times\cdots\times G_s$

习　　题　　58

1.如果η是一个正规自同态，求证：η的形状是$a\eta=c(a,\eta)a$，这里$c(a,\eta)$是与$G\eta$的各元素可交换的一个元素，并且$c(ab,\eta)=c(a,\eta)[ac(b,\eta)a^{-1}]$。

证：$\because\eta$是G的一个正规自同态，对$\forall x$，$a\in G$，有
$(aC_x)\eta=(a\eta)C_x$，即$(x^{-1}ax)\eta=x^{-1}(a\eta)x$

命$c(a,\eta)=(a\eta)a^{-1}$，我们来证明$c(a,\eta)$适合题目要求

显然有$a\eta=(a\eta)a^{-1}\cdot a=c(a,\eta)a$，且

(1)对$\forall x\eta\in G\eta$，有$c(a,\eta)(x\eta)=(x\eta)c(a,\eta)$

$\because c(a,\eta)(x\eta)=(a\eta)a^{-1}(x\eta)=(a\eta)a^{-1}(x\eta)a\cdot a^{-1}=(a\eta)[a^{-1}(x\eta)a]a^{-1}=(a\eta)[(a^{-1}xa)\eta]a^{-1}=(a\eta)(a\eta)^{-1}(x\eta)(a\eta)a^{-1}$
$=(x\eta)(a\eta)a^{-1}=(x\eta)c(a,\eta)$

(2) $c(ab, \eta) = c(a, \eta)[ac(b, \eta)a^{-1}]$

$\because (ab)\eta = c(ab, \eta)(ab)$, $\therefore c(ab, \eta) = (ab)\eta$

$(ab)^{-1} = (ab)\eta b^{-1}a^{-1} = (a\eta)(b\eta)b^{-1}a^{-1}$

$= (a\eta)a^{-1} \cdot a(b\eta)b^{-1}a^{-1} = c(a, \eta)[ac(b, \eta)a^{-1}]$

2.如果心$C = 1$，或者换位子群$G^{(1)} = G$（参看习题51第3题定义），求证：恒等映照是G的唯一正规自同构。

证：1）$C = 1$时，设η是G的正规自同构，当然是G的正规自同态，依上题有$\forall a \in G$：$a\eta = c(a, \eta)a$，又因$G\eta = G$，$\therefore c(a, \eta) \in C$，因$C = 1$，即$c(a, \eta) = 1$，得$a\eta = a$，故$\eta$是G的恒等映照。

2）$G^{(1)} = G$时，设η是G的正规自同构，则$G\eta = G$。对$\forall a \in G$，$c(a, \eta)$与G中任一元可交换，故$c(ab, \eta) = c(a, \eta)[ac(b, \eta)a^{-1}] = c(a, \eta)c(b, \eta) = c(b, \eta)c(a, \eta)$

对G中任意元a，由$G^{(1)} = G$，必存在$b, d \in G$，使$a = bdb^{-1}d^{-1}$

由题1知$a\eta = c(a, \eta)a$

但$c(a, \eta) = c(bdb^{-1}d^{-1}, \eta) = c(b, \eta)c(d, \eta)c(b^{-1}, \eta)c(d^{-1}, \eta) = c(bb^{-1}dd^{-1}, \eta) = c(1, \eta)$

$\because 1\eta = 1 = c(1, \eta) \cdot 1$ $\therefore c(1, \eta) = 1$

即$c(a, \eta) = 1$ $\therefore a\eta = a$，即η是G的恒等映照

3.令$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$是一个直接分解的射影。如果$i_1, i_2, \cdots i_r$不相同，求证：$\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}$是一个自同构，并求证：$\varepsilon_i + \varepsilon_j = \varepsilon_j + \varepsilon_i$。

证：设$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$是直接积$G = G_1 \times G_2 \times \cdots \times G$的射影。依定义，对G中任意元$x = x_1 x_2 \cdots x_n$,

$x_i \in G_i$，有 $x\varepsilon_i = x_i (i = 1, 2, \cdots, n)$

(1) $\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}$ 是G的一个自同态。

$\forall x \in G, \ x = x_1 x_2 \cdots x_n, \ x_i \in G_i$

$x(\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}) = (x\varepsilon_{i_1})(x\varepsilon_{i_2})\cdots$
$(x\varepsilon_{i_r}) = x_{i_1} x_{i_2} \cdots x_{i_r} \in G$

又$\forall y \in G, \ y = y_1 y_2 \cdots y_n, \ y_i \in G_i$

$(xy)(\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}) = [(xy)\varepsilon_{i_1}][(xy)$
$\varepsilon_{i_2}]\cdots[(xy)\varepsilon_{i_r}] = (x_{i_1} y_{i_1})(x_{i_2} y_{i_2})\cdots$
$(x_{i_r} y_{i_r}) = (x_{i_1} x_{i_2} \cdots x_{i_r})(y_{i_1} y_{i_2} \cdots y_{i_r})$
$= x(\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}) y(\varepsilon_{i_1} + \varepsilon_{i_2} +$
$\cdots + \varepsilon_{i_r})$

$\forall m \in M$

$(xm)(\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}) = (x_{i_1} m)(x_{i_2} m)\cdots$
$(x_{i_r} m) = (x_{i_1} x_{i_2} \cdots x_{i_r}) m$
$= x(\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_r}) m$

(2) $\varepsilon_i + \varepsilon_j = \varepsilon_j + \varepsilon_i$

$\because x(\varepsilon_i + \varepsilon_j) = (x\varepsilon_i)(x\varepsilon_j) = x_i x_j = x_j x_i$
$= (x\varepsilon_j)(x\varepsilon_i) = x(\varepsilon_j + \varepsilon_i)$

习　题　59

1. 令G适合Ⅰ′及Ⅱ′，并令η是一个正规自同态。令r是第一个整数能使$G\eta^r = G\eta^{r+1}$，并令s是第一个整数能使$Z_s = Z_{s+1}$，这里Z_i是η^i的核。求证：$r = s$。

证：根据费廷（Fitting）引理。令$H = G\eta^r$，$R = Z_s$，则有$G = R \times H$，且$H\eta = H$。

今证$r = s$，对$\forall x \in G$，有$x = x_1 x_2$，$x_1 \in R$，x_2

$\in H$

则$x\eta^r=(x_1\eta^r)(x_2\eta^r)\in H$，又因为$H\eta=H$，$R\eta\subseteq R$。

$(x_1\eta^r)=(x\eta^r)(x_2\eta^r)^{-1}\in H$，$x_1\eta^r\in R$。由$R\cap H=1$得

$x_1\eta^r=1$，且当x取遍G中所有元时，x_1也必须取遍R中所有元。

于是对任一$x_1\in R$，有$x_1\eta^r=1$，$\therefore r\geq s$

又$x_1\eta^s=(x_1\eta^s)(x_2\eta^s)=1\cdot(x_2\eta^s)=x_2\eta^s\in H$

即$G\eta^s\subseteq H=G\eta^r$，$\therefore r\leqslant s$，于是得$s=r$。

习　题　60

在下面各题里假定不变M—子群的两个链条件都成立。

1.如果G的心=1，或者$G=G^{(1)}$，求证：G只有一种分解成不可分解群的直接积。

证：设G有两种分解成不可分解群的直接积：

$G=G_1\times G_2\times\cdots\times G_s$

$G=H_1\times H_2\times\cdots\times H_t$

则根据Krull-Schmidt定理知，有$s=t$，并且把H_i的次序适当排列后，有G的一个正规自同构μ存在，使$G_i\mu=H_i$（$i=1,2,\cdots,s$）。

由习题58第2题知，此时G的正规自同构只有恒等映照，即$\mu=1$，于是$G_i=H_i$（$i=1,2,\cdots,s$）。所以G只有一种分解。

2. 令ξ_1，ξ_2，$\cdots\xi_s$又η_1，η_2，$\cdots$，η_s是由G分解为不可分解群的两种直接分解所决定的射影。如果适当地选取η的次序，求证：必有一个正规自同构μ存在，使$\eta_i=\mu^{-1}\xi_i\mu$ $(i=1, 2, \cdots, s)$

证：设$G=G_1\times G_2\times\cdots\times G_s$　　　　(1)

$$G=H_1\times H_2\times\cdots\times H_s \qquad (2)$$

是G分解为不可分解群的两种直接分解，由克鲁尔—叔密特定理知将H_i的次序适当编排后，则有一个正规自同构μ存在使$G_i\mu=H_i(i=1, 2, \cdots, s)$。∴若$x\in H_i$则$x\mu^{-1}\in C_i$

又设(1)和(2)所对应的射影分别为ξ_1，ξ_2，$\cdots$，ξ_s及η_1，η_2，$\cdots$，η_s，则对任意$x\in G$，有

$$x=x_1x_2\cdots x_s,\ x_i\in H_i,\ i=1, 2, \cdots, s$$

$$\begin{aligned}\therefore x_1\mu^{-1}\xi_i\mu &= (x_1x_2\cdots x_s)\mu^{-1}\xi_i\mu\\ &=(x_1\mu^{-1}x_2\mu^{-1}\cdots x_s\mu^{-1})\xi_i\mu=(x_i\mu^{-1})\mu\\ &=x_i=x\eta_i\end{aligned}$$

即$\eta_i=\mu^{-1}\xi_i\mu(i=1, 2, \cdots, s)$

3. 如果群G的不可分解的因子是同构的，则G叫做齐次群。如果射影ε使$G\varepsilon$是不可分解群。则这ε叫做原射影。令ε及ε'是齐次群的原射影，求证：必有一个正规M—自同构μ存在，使$\varepsilon'=\mu^{-1}\varepsilon\mu$。

证：因为G是齐次群，由原射影ε及ε'所决定的不可分解群$G\varepsilon$与$G\varepsilon'$互相同构。故有一个正规M—自同构μ存在，使$G\varepsilon\mu=G\varepsilon'$。依上题知，此时有$\varepsilon'=\delta^{-1}\varepsilon\mu$。

习　题　61

1.令G是一个交换群，没有无限价的元素，对于每个素数p，令Gp是由价数等于p的幂的元素所构成的子集合。求证：Gp是G的一个子群，并且$G=\underset{p}{\pi}Gp$。

证：∀a，b∈Gp，设$a^{p^n}=1$，$b^{p^m}=1$，取$t=\max(n, m)$。

则有$(ab)^{p^t}=a^{p^t}\cdot b^{p^t}=1$，∴ab∈Gp。

又$(a^{-1})^{p^n}=(a^{p^n})^{-1}=1$，∴$a^{-1}\in Gp$。于是Gp是G的子群

其次，对任一g∈G，设g的阶数是n，若$n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$，其中$p_i$是素数，且i≠j时$p_i\neq p_j$，则$g\in Gp_1Gp_2\cdots Gp_s$。

依无限直接积的定义，即得$G=\underset{p}{\pi}Gp$。

2.如果前题里所考究的群G是一个环的加法群，求证：Gp是理想，所以环G是直接和$\underset{p}{\Sigma}\oplus Gp$。并且当p≠q时，GpGq＝0

证：∵Gp＝{a | a的阶数为p的幂，a∈G，p为素数}

∴∀a，b∈G，设$p^{\alpha}a=0$，$p^{\beta}b=0$

则$p^{\alpha+\beta}(a-b)=p^{\alpha+\beta}a-p^{\alpha+\beta}b=p^{\beta}(p^{\alpha}a)-p^{\alpha}(p^{\beta}b)=0$

对∀g∈G，有$p^{\alpha}(ag)=(p^{\alpha}a)g=0$由此知a－b的

阶$l \mid p^{\alpha+\beta}$，ag的阶$n \mid p^{\alpha}$，故$l=p^k$，$n=p^t$．

即$a-b\in G_p$，$ag\in G_p$，相仿可证$ga\in G_p$。

$\therefore G_p$是G的理想，故$G=\sum\limits_{p}\oplus G_p$

其次，若$p\neq q$，设$x\in G_pG_q$

则$x=ab$，$a\in G_p$，$b\in G_q$，$\therefore p^{\alpha}a=q^{\beta}b=0$

$p^{\alpha}x=p^{\alpha}(ab)=(p^{\alpha}a)b=0$，$q^{\beta}x=q^{\beta}(ab)=a(q^{\beta}b)=0$

若x的阶是l，则$l \mid p^{\alpha}$，$l \mid q^{\beta}$，于是$l=p^t=p^u$（$0\leqslant t\leqslant \alpha$，$0\leqslant u\leqslant \beta$）又$\because (p, q)=1$，$\therefore t=u=0$，即$l=1$，$\therefore x=0$，故$G_pG_q=0$（$p\neq q$）

3．令G是一个M—群，并令$\{R_\alpha\}$是G里不变M—子群的集合，能使$\bigcap R_\alpha=1$，求证：G同构于群$G_\alpha=G/R_\alpha$的一个子直接和。

〔证法一〕命v_α是G到$G_\alpha=G/R_\alpha$上的自然M—同态。显然$\overline{\pi}G_\alpha$是群G_α的一个子直接和，记为$G'=\overline{\pi}G_\alpha$

今证$G\cong G'$。

$\forall g\in G$，令映照$g\to \pi g_\alpha$，其中$g_\alpha=gv_\alpha$，是G到G'上的映照，且g，$h\in G$

$gh\to \pi(gh)_\alpha=\pi g_\alpha h_\alpha$ $\because (gh)_\alpha=(gh)v_\alpha$

$=(gv_\alpha)(hv)_\alpha=g_\alpha h_\alpha$

$m\in M$，$gm\to \pi(gm)_\alpha=\pi g_\alpha m\because (gm)v_\alpha=gv_\alpha$

$\cdot m \cong g_{\alpha} \cdot m$

所以映照$g \to \pi g_{\alpha}$是G到G′上的M—同态。

今求其同态核，由$\pi g_{\alpha} = 1$，即对所有a：$g_{\alpha} = 1$，于是，对所有α，$g \in R_{\alpha}$，由条件$\bigcap R_{\alpha} = 1$，得出$g = 1$，即同态核 = 1，所以$G \cong G'$

〔证二〕作G到$\pi_{\alpha} G_{\alpha}$内的映射η：$a \to A(\alpha) = aR_{\alpha}$

（这里A(α)实际上是α的函数）

又$(ab)\eta \overset{记}{=} F(\alpha) = (ab)R_{\alpha} = (aR_{\alpha})(bR_{\alpha}) = A(\alpha)B(\alpha) = (a\eta)(b\eta)$

∴η是同态映射。（η的单值性显然）

又 ∵$\eta^{-1}(1') = \bigcap R_{\alpha} = 1$ ∴η是同构映射。

又∵Gη到G_{α}内的映射ξ：$h \to h(\alpha)$，显然有$(G\eta)\xi = G\alpha$

∴Gη是$G_{\alpha} = G/R\alpha$的一个子直接积

即G同构于群$G\alpha = G/G\alpha$的一个子直接积Gη。

第六章　模及理想

习　题　62

1．如果I是A的一个左理想，令IM表示有限和$\sum b_i x_i$的集合，这里$b_i \in I$，$x \in M$。求证IM是M的一个子模。

〔证明〕首先设$p \in IM$及$q \in IM$。即$p = \sum b_i x_i$，$q =$

$\sum b_j x_j$，其中b_i，$b_j \in I$，$x_i, x_j \in M$。

则$p - q = \sum b_i x_i - \sum b_j x_j = \sum b_i x_i + \sum(-b_j)x_j = \sum b_l x \in IM$故$IM$是$M$的子群。

其次设$M \in A$，$p = \sum b_i x_i \in IM$，则$ap = a\sum b_i x_i = \sum(ab_i)x_i = \sum b'_i x_i \in IM$（∵是A的左理想，∴若$a \in A$，$b_i \in I$则$ab_i = b_i' \in I$）因此由定义可知IM是M的一个子模。

2．如果I是A的一个右理想，求证：对于I里所有b能使$by = 0$的元素y（$\in M$）的全体是一个子模。

〔证明〕：首先记$N = \{y \mid y \in M$，且对任意的$b \in I$有$by = 0\}$

设y_1，$y_2 \in N$，即对任意的$b \in N$有$by_1 = 0$，$by_2 = 0$。于是$b(y_1 - y_2) = by_1 - by = 0$，故$y_1 - y_2 \in N$。即N是M的子群。

其次对任意的$a \in A$，$y \in N$可证$ay \in N$。事实上，对于任意的$b \in N$。因为I是A的右理想，所以$ba \in I$。因此$b(ay) = (ba)y = 0$。所以$ay \in N$。由定义即知N是M的子模。

3．令A是带恒等元素1的环。求证：任一个A一模可有一个表示$M = 1M \oplus N$，这里1M是元素1x的子模，而N是被A里每个a所零化的元素构成的子模。

〔证明〕首先对于任意的$g \in M$，令$g = 1g + g'$，显然$1g \in 1M$。且有$g' \in N$，这是因为对任意的$a \in A$，$ag = a(1g + g') = (a \cdot 1)g + ag' = ag + ag'$所以$ag' = 0$。因而$g' \in N$于是$M = 1M + N$。

其次，显然M中元素0的此种表示法是唯一的。事实上由$0 = 1 \cdot 0 + g' = 0 + g'$得$g' = 0$，于是$0 = 0 + 0$。故$M = 1M + N$是直和。即$M = 1M \oplus N$。

而1M和N是子模是显然的。

4．整数环里下面的商：

(6):(3)，(6):(15)，(3):(9)

是什么？

〔解〕由定义可得(6):(3)=(2)，(6):(15)=(2)

(3):(9)=I（整数环）

5．证明：关于商的下面法则：

(a)如果$N_1 \supseteq N_2$，则$N_1 : N_2 = A$

(b)$(N_1 \cap N_2 \cap \cdots \cap N_k) : N = N_1 : N \cap N_2 : N \cap \cdots \cap N_k : N$。

(c)$N_1 : N_2 = N_1 : (N_1 + N_2)$

〔证明〕(a)因为N_2是M的A—子模，所以对任意的$c \in A$，有$cN_2 \subseteq N_2$，因而$cN_2 \subseteq N_1$。由定义$N_1 : N_2 = A$。

(b)设$c \in (N_1 \cap N_2 \cap \cdots \cap N_k) : N$，则$cN \subseteq N_1 \cap N_2 \cap \cdots \cap N_k$，因此$cN \subseteq N_1$，$cN \subseteq N_2 \cdots cN \subseteq N_k$。从而$c \in N_1 : N$，$c \in N_2 : N$，…，$c \in N_k : N$

所以$c \in N_1 : N \cap N_2 : N \cap \cdots \cap N_k : N$。

相反的过程也成立，所以$(N_1 \cap N_2 \cap \cdots \cap N_k) : N$
$= N_1 : N \cap N_2 : N \cap \cdots \cap N_k \cap N$。

(c)设$c \in N_1 : N_2$，则$cN_2 \subseteq N_1$，因为$cN_1 \subseteq K_1$，所以$cN_1 + cN_2 \subseteq N_1$即$c \in N_1 : (N_1 + N_2)$，故$N_1 : N_2 \subseteq N_1 : (N_1 + N_1)$

反之，设$c \in N_1 : (N_2 + N_1)$，则$c(N_1 + N_2) \subseteq N_1$，所以$cN_2 \subseteq N_1$，即$c \in N_1 : N_2$，所以$N_1 : N_2 \supseteq N_1 : (N_1 + N_2)$，

于是$N_1 : N_2 = N_1 : (N_1 + N_2)$

6．若$N_1 \subseteq N_2$，则$N_1 : N_2 = 0 : (N_2 - N_1)$

〔证明〕注意到这里$N_2 - N_1$表示差模，而0是$N_2 - N_1$中的零元。首先设$c \in 0 : (N_2 - N_1)$则对任意的$n_2 \in N_2$成立$c(n_2 + N_1) \subseteq N_1$．因而$c(N_2 + N_1) \subseteq N_1$，$cN_2 + cN_1 \subseteq N_1$于是$cN_2 \subseteq N_1$即$c \in N_1 : N_2$。

反之，设$c \in N_1 : N_2$，则$cN_2 \subseteq N_1$，$c(N_2 + N_1) \subseteq N_1$即$c \in 0 : (N_2 - N_1)$。因此$N_1 : N_2 = 0 : (N_2 - N)_1$。

7．如果A是带恒等元素环，求证：$I : A$是含在左理想I里的A的最大双侧理想。

〔证明〕先证$I : A$是A的双侧理想。设x，$y \in I : A$，则$xA \subseteq I$，$yA \subseteq I$，故$(x - y)A = xA - yA \subseteq I$。从而$x - y \in I : A$。又，若$a \in A$则有$axA \subseteq aI \subseteq I$。所以$ax \in I : A$，又由$xaA \subseteq xA \subseteq I$可得$xa \in I : A$，于是$I : A$是A的双侧理想。

次证$I : A \subseteq I$。设$x \in I : A$，则$xA \subseteq I$，但A中有恒等元素e，使$xe = x$。所以$x = xe \in I$。于是$A \subseteq I$。

最后证$I : A$是最大双侧理想。

设$I : A$不是I里A的最大双侧理想。则另有一个A的双侧理想R存在，满足$R \subseteq I$而$I : A \subset R$（真包含）故必有元素$r \in R$而$r \in I : A$。因为$r \in R$，所以$rA \subseteq R \subseteq I$于是$r \in I : A$与关于r的条件矛盾，故所设的R不存在，从而$I : A$为I里A的最大双侧理想。

习　题　63

1．如果I是左理想，而有一个元素e存在使$xe \equiv x \pmod{I}$对于A里所有x成立，则I叫做正侧左理想。如果M是一

个单式循环模，求证：$M\cong A-I$，这里I是一个适宜的正则左理想。

〔证明〕由定义知M是由一个元素生成的．且$AM=M$，于是有元素$x\in M$，使M中任意元都可表为ax，$a\in A$。

今考察同态映射$\sigma: a\to ax$。这是将A看作左A模到左A模M上的A—同态。将σ的核$\{a\mid ax=0, a\in A\}$记为I。显然I是A的左理想，也可视为左A子模。于是$M\cong A-I$。

下面证明I是正则左理想。因为σ是A到M上的A-同态，特别x也有原象e，使$\sigma: e\to ex=x$，故$x-ex=0$。因此对任意的$a\in A$，$a(x-ex)=ax-aex=(a-ae)x=0$。所以$a-ae\in I$，即$ae\equiv a(\mathrm{mod} I)$于是I是A的正则左理想。

2．如果I是正则的，求证$I\supseteq I:A$。

〔证明〕设$x\in I:A$，则$xA\subseteq I$。因为I是正则理想，故有$e\in A$．使得$xe\equiv x(\mathrm{mod} I)$，即$xe-x\in I$。又因为$xA\subseteq I$．所以$xe\in I$从而有$x\in I$．于是$I\supseteq I:A$。

3．令M是一个单纯A—模，求证：或者$AM=0$，这时M是有限模，所含元素的个数是素数；或者M是一个单式循环模，以非零元素为生成元。求证它的逆定理：如果这两个条件中有一个成立，则M是单纯模。

〔证明〕由M是单纯A一模，知AM是M的A一子模，所以只有两种情况：

或者$AM=0$，此时对M的任意子模N，都有$AN=0$，因而都是A一子模。因为M是单纯A一模，故M是可换单纯群。因此M必是素数阶的循环群。

或者$AM=M$。此时首先因M是单式模，若在M中取$x\neq 0$，则由x生成的A一子模$N\neq 0$，故必有$N=M$。因此M可

视为由x生成的循环群。显然，M中任一个非零元素均可作为生成元。

逆定理证明如下：

对第一种情况，由AM＝0，可知M没有真子模，故M是单纯A一模；对第二种情况，因为M是单式循环模，设N是M的非零A一子模，则N中有非零生成元素x，但由此x生成的A一子模就应该是M，故M＝N，这样M是单纯A一模。

习 题 64

1 如果只就升链条件而论，求证，定理3里关于M是单式模的假定是多余的。即如果A是一个环，适合关于左理想的升链条件，则任一个有限生成的A模M适合关于子模的升链条件。

〔证〕令x_1，x_2，…，x_r是M的生成元的一个固定集合，N是M的任一个子模。则N的每一个元素可表示成$a_1x_1+\cdots+a_rx_r+m_{r+1}x_1+\cdots+m_{2r}x_r$。其中$a_i\in A$。$(i=1,2,\cdots,r)$ $m_{r+i}\in I$（整数环）$i=1,2,\cdots,r$。

若 $b_jx_j+b_{j+1}x_{j+1}+\cdots+b_rx_r+n_{r+1}x_1+\cdots+n_{2r}x_r\in N$

记这种b的全体为$I_j(N)$．$(j=1,2,\cdots,r,r+1,\cdots,2r)$．显然$I_j(N)$当$1\leqslant j\leqslant r$时是环A的一个左理想，当$r+1\leqslant j\leqslant 2r$时是整数环I的一个左理想。並且当N，P都是M的子模且$N\subseteq P$时，有$I_j(N)\subseteq I_j(P)$。$(j=1,2,\cdots,r,r+1,\cdots,2r)$．类似引理1的证明：当$N\subseteq P$，且对所有j，$I_j(N)=I_j(P)$，则可推得$N=P$。由于整数环是主理想整区，所以适合关于理想的升链条件。

今令$N_1\subseteq N_2\subseteq\cdots$是M的子模的一个升链，则伴随着这

个链可得2r个左理想链。

$I_j(N_1)\subseteq I_j(N_2)\subseteq\cdots\cdots$ ($j=1,2,\cdots,r,r+1,\cdots,2r$)

由于升链条件在A与I里成立，则对每个j可得一个整数l_j，使$I_j(N_{l_j})=I_j(N_{l_j+1})=\cdots$ ($j=1,2\cdots,2r$)

取$l=\max(l_1,l_2,\cdots,l_{2r})$，则$I_j(N_l)=I_j(N_{l+1})=\cdots$ ($j=1,2,\cdots,2r$)。类似于引理1，可推得 $N_l=N_{l+1}=\cdots$。

2。如果A带有恒等元素，並且A的各个左理想是有限生成的。

求证：环A上x的幂级数环A〈x〉（参看习题39的第1题）里各个左理想是有限生成的。

〔证明〕因为A可视为单式A—模，且其每一个左理想，也即每一个A—子模是有限生成的。由本章定理2可知A适合关于子模的升链条件。

设B是A〈x〉的任一左理想，$I_j(B)$是满足$b_0+b_1x+b_2x^2+\cdots+bx^j+ox^{j+1}+ox^{j+2}+\cdots\in B$的A中的元素b的全体所组成的集合。因为B是左理想，所以$I_j(B)$也是A的左理想。且显然$I_j(B)\subseteq I_{j+1}(B)$（因为$x(b_0+b_1x+\cdots+bx^j+0+\cdots)=b_0x+b_1x^2+\cdots+bx^{j+1}\in B$）故$I_0(B)\subseteq I_1(B)\subseteq\cdots$存在某一整数N，使得$I_N(B)=I_{N+1}(B)=\cdots=I(B)$。因为$I(B)$是A的左理想，由题设$I(B)$是有限生成的。令$I_i(B)=(b_{i1},b_{i2},\cdots,b_{in_i})$ $i=0,1,2\cdots N$

记$f_{ij}(x)=a_0+a_1x+\cdots+b_{ij}x^i+o\cdot x^{i+1}+ox^{i+2}+\cdots\in B$则$(f_{01},f_{02}\cdots f_{0n_0},f_{11}\cdots f_{1n_1},f_{21},\cdots f_{Nn_N})=B$也即，B是有限生成的。用归纳法证明如下：

首先B中形如$b_0+ox+ox^2+\cdots$的元素可由$f_{01},f_{02}\cdots f_{0n_0}$表

示。这是因为$b_0+ox+ox^2+\cdots\in B$，所以$b_0\in I_0(B)$即$b_0=\sum_{i=1}^{n_0}a_ib_{0i}$，$a_i\in A$。因此$b_0+ox+ox^2+\cdots=\sum_{i=1}^{n_0}a_if_{0i}$。

其次，假设B中形如$a_0+a_1x+a_2x^2+\cdots+a_rx^r+ox^{r+1}+\cdots$的元素已可由$(f_{01},f_{02}\cdots f_{Nn_N})$表示。今证形如$b_0+b_1x+\cdots+b_{r+1}x^{r+1}+ox^{r+2}+\cdots$也可由$(f_{01},f_{02}\cdots f_{Nn_N})$表示。

(i)若$r+1<N$，即$b_{r+1}\in I_{r+1}(B)$因此$b_{r+1}=\sum_{i=1}^{n_{r+1}}c_ib_{r+1i}$则$(b_0+b_1x+\cdots+b_{r+1}x^{r+1}+ox^{r+2}+\cdots)-\sum_{i=1}^{n_{r+1}}c_if_{r+1i}=b_0'+b_1'x+\cdots+b_r'x^r+ox^{r+1}+ox^{r+2}+\cdots$因为$\sum_{i=1}^{n_{r+1}}c_if_{r+1i}\in B$，故$b_0'+b_1'x+\cdots+b_r'x^r+ox^{r+1}+\cdots\in B$由归纳法假设即得$b_0+b_1x+\cdots+b_{r+1}x^{r+1}+ox^{r+2}+\cdots$可由$(f_{01},f_{02}\cdots f_{Nn_N})$表示。

(ii)若$r+1>N$，即$b_{r+1}\in I_N(B)$设$b_{r+1}=\sum_{i=1}^{n_N}c_i'b_{Ni}$

由此得$(b_0+b_1x+\cdots+b_{r+1}x^{r+1}+ox^{r+2}+\cdots)-x^{r-N}\sum_{i=1}^{n_N}c_i'f_{Ni}=a_0'+a_1'x+\cdots+a_r'x^r+ox^{r+1}$。因此$b_0+b_1x+\cdots+b_{r+1}x^{r+1}+ox^{r+2}\cdots$可由$(f_{01},f_{02}\cdots f_{Nn_N})$表示。

故B是有限生成的，于是命题得证。

8．令F是含有q个元素的一个有限域，并令Z是F[x_1，

$x_2\cdots x_r$〕里多项式$m(x_1,x_2\cdots x_r)$的理想，它对于F里所有s_i使$m(s_1\cdots s_r)=0$。求决定Z的生成元素所成的有限集合。

〔证明〕首先Z是F〔$x_1\cdots x_r$〕的理想是显然的。

事实上，若$m_1(x_1\cdots x_r)$，$m_2({}_1x\cdots x_r)\in Z$则$m_1(x_1,x_2\cdots x_r)-m_2(x_1-x_r)\in Z$。这是因为$m_1(s_1,s_2\cdots s_r)-m_2(s_1,s_2\cdots s_r)=0$对于所有$s_i\in F$成立

又若$f(x_1\cdots x_r)\in F$〔$x_2x_2\cdots x_r$〕则$f(x_1\cdots x_r)m_1(x_1\cdots x_r)=m_1(x_1\cdots x_r)f(x_1\cdots x_r)\in Z$。这是因为$f(s_1,\cdots s_r)m_1(s_1\cdots s_r)=0$对所有$s_i\in F$成立。

其次，由Hilbert基定理的系2可知F〔$x_1,x_2\cdots x_r$〕的每一理想都是有限生成的，故Z是有限生成的。

设F里的全体元素为$s_1,s_2\cdots\cdots s_q$。则Z的生成元为

$$\prod_{i=1}^{q}(x_1-s_i),\quad \prod_{i=1}^{q}(x_2-s_i),\cdots \prod_{i=1}^{q}(x_r-s_i)$$

习 题 65

1．如果$q\neq 0,1$求证：（g）是I的准素理想必须且只须$q=p^c$。这里p是一个素数。

〔证明〕充分性：设$q=p^e(q\neq 0,1)$若$ab\equiv 0\ (\mathrm{mod}(p^e))$ $b\not\equiv 0\ (\mathrm{mod}(p^e))$，即$b=p^{\alpha}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ p,p_i是素数。$0\leqslant\alpha<e,s\geqslant 0$，另一方面由$ab\equiv 0\ (\mathrm{mod}\ (p^e))$得$ab=mp^e$因而$a=\dfrac{mp^e}{b}=m'p^{e-\alpha}$，$e-\alpha>0$。故存在整数r，使得$a^r\equiv 0\ (\mathrm{mod}(p^e))$因此$a\equiv 0\ (\mathrm{mod}R(p^e))$。由定义即知$(p^c)$是准素理想。

必要性：设$q\neq 0,1$，(q)是I的准素理想。由准素理想

的直接推论知准素理想的根集是素理想，而I是主理想环，故(q)的根集R((q))=(p)。p是某一个素数。

若$ab\equiv 0 \pmod{(q)}$，$b\not\equiv 0 \pmod{(q)}$则$a\equiv 0 \pmod{(p)}$。又由$a^r\equiv 0 \pmod{(q)}$，r是某一整数。得$a^r=nq$。又因$a=mp$所以$m^rp^r=nq$因此$q=\frac{m^r}{n}p^r$。即$q=sp^e$，e，s是整数。今证s=1或pα。若s≠1或pα则$s=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{s'}^{\alpha_{s'}}$，$p_1\neq p$，$s'\geqslant 1$，$p_i$是素数且当$i\neq j$时$p_i\neq p_j$。于是$q=p^ep_1^{\alpha_1}\cdots p_s^{\alpha_s}$，因而应有$R((q))=(pp_1p_2\cdots p_{s''})\neq(p)$这与R((q))=(p)矛盾。故s=1或pα则$q=p^e$。e是整数。

2．如果B是一个素理想，并且C_1及C_2是使$C_1C_2\equiv 0$ (modB)的理想，求证$C_1\equiv 0$ (modB)或$C_2\equiv 0$ (modB)

〔证明〕由题设$\forall c_1\in C_1$，$c_2\in C_2$有$c_1c_2\in C_1C_2\equiv 0$ (modB)。因此$c_1c_2\equiv 0$ (modB)。因为B是素理想。故若$c_2\not\equiv 0$ (modB)必有$c_1\equiv 0$ (modB)因而$C_1\equiv 0$ (modB)；同理若$c_1\not\equiv 0$ (modB)必有$c_2\equiv 0$ (modB)因而$C_2\equiv 0$ (modB)。

3．求证：$R(B_1\cap B_2)=R(B_1)\cap R(B_2)$

〔证明〕设$x\in R(B_1\cap B_2)$则有正整数p，使$x^p\in B_1\cap B_2$即$x^p\in B_1$，且$x^p\in B_2$。故$x\in R(B_1)$且$x\in R(B_2)$从而得$x\in R(B_1)\cap R(B_2)$

反之，设$y\in R(B_1)\cap R(B_2)$则$y\in R(B_1)$且$y\in R(B_2)$因而有正整数k与l，使$y^k\in B_1$，$y^l\in B_2$。令r=max(l,k)则有$y^r\in B_1\cap B_2$。故$y\in R(B_1\cap B_2)$

于是$R(B_1\cap B_2)=R(B_1)\cap R(B_2)$

4．求证：$B_1^r \subseteq B_2$在一个诺德环里成立必须而且只须$R(B_1) \subseteq R(B_2)$。

〔证明〕必要性：设$x \in R(B_1)$则存在整数p使$x^p \in B_1$，从而$x^{pr} \in B_1^r \subseteq B_2$。故$x \in R(B_2)$，所以$R(B_1) \subseteq R(B_2)$。

充分性：设$x \in R(B_1)$，则$x \in R(B_2)$。故必有整数p,q存在，使$x^p \in B_1$，$x^q \in B_2$。因为$R(B_2)$关于B_2是幂零的。即存在整数r，使$R^r(B_2) \subseteq B_2$。又$B_1 \subseteq B_1$ (R) 所以$B_1^r \subseteq R^r(B_1) \subseteq R^r(B_2) \subseteq B_2$。于是得$B_1^r \subseteq B_2$。

习 题 66

1．求把(x^2, xy)写成有限个准素理想的交。

〔解〕首先因为$x \notin (x^2, xy)$，$y \notin R((x^2, xy)) = (x)$而$xy \in (x^2、xy)$．由准素理想定义知$(x^2, xy)$不是准素理想。又因为$(x^2, xy):(y) = (x)$。$(x^2, xy):(y^2) = (x)$
所以$(x^2, xy) = (x) \cap ((x^2, xy) + (y^2)) = (x) \cap (x^2, xy, y^2)$因为$(x)$是素理想故必为准素理想．下面证明$(x^2, xy, y^2)$也是准素理想。事实上$xy \equiv 0 \pmod{(x^2, xy, y^2)}$，虽然，$y \notin (x^2, xy, y^2)$)，但$x \in R(x^2, xy, y^2)$虽然$x \notin (x^2, xy, y^2)$但$y \in R(x^2, xy, y^2)$对于$(x^2, xy, y^2)$中其他形式的元素，定义的条件必然满足，故$(x^2, xy, y^2)$是准素理想。

2．求证：理想(x^2, xy, y^2)是准素理想，并且在F〔x, y〕里是可约的。

〔证明〕上题已证(x^2, xy, y^2)是准素理想。下证其为可约的。

因为$(x^2, xy, y^2) = (x^2, xy, y) \cap (x, xy, y^2)$

显然$(x^2, xy, y) \supset (x^2, xy, y^2)$，因$y \in (x^2, xy, y)$而$y \notin$

(x^2,xy,y^2)

同理$(x,xy,y^2)\supset(x^2,xy,y^2)$因$x\in(x,xy,y^2)$而$x\bar{\in}(x^2,xy,y^2)$

故(x^2,xy,y^2)是可约的。由此可知准素理想不一定是不可约的。

3．求证费廷定理：令M是一个A—模（A是任意的）适合升链条件，设有M的一个A—自同态θ存在，它不是无势的，也不是M的一个同构，则M里存在有两个子模$M_i\neq 0$（$i=1,2$），使$M_1\cap M_2=0$

〔证〕：记$N_i=\{x\mid x\in M;\ x\theta^i=0\}$，显然$N^i$是M的一个子模。且$N_i\subseteq N_{i+1}$.（$i=1,2\cdots$），∵对$\forall x\in N_i$，有$x\theta^i=0$。∴$x\theta^{i+1}=(x\theta^i)\theta=0\theta=0$即$x\in N_{i+1}$.于是$N_1\subsetneq N_2\subseteq\cdots$是M的子模的一个升链．故存在一正整数k，使$N_k=N_{k+1}=\cdots$。

命$M_1=N_k$．因θ不是M的一个同构，所以$M_1\neq 0$．再命$M_2=M\theta^k$，因θ不是无势的．即$\theta^k\neq 0$．故$M_2\neq 0$．显然M_2是M的一个子模．且满足$M_1\cap M_2=0$．∵对任一$x\in M_1\cap M_2$．即$x\in M_1$，$x\theta^k=0$．又$x\in M_2$.∴存在$y\in M$，使$x=y\theta^k$，于是$x\theta^k=(y\theta^k)\theta^k=y\theta^{2k}=0$即$y\in N_{2k}=N_k$，得$x=y\theta^k=0$．

4．求证费廷定理：令M是适合升链条件的一个A—模设M的任意两个非零模的交$\neq 0$．则M的无势A—自同态的集合是A—自同态环E里一个理想R．如果$\alpha\in E$是一个左零因子，则$\alpha\in R$.

〔证〕：设R是M的无势A—自同态的集合．今证R有E的理想。对$\forall\theta_1,\theta_2\in R$,则$\theta_1-\theta_2$仍是M的一个A—自

同态。且$\theta_1-\theta_2$不是M的一个同构。∵θ_1，θ_2都是无势的. ∴θ_1，θ_2都不是M的同构. 记，$N_1(\theta_1)=\{x\mid x\in M, x\theta_1=0\}$，$N_2(\theta_2)=\{x\mid x\in M, x\theta_2=0\}$. 它们都是M的非零子模. 依假设有$N_1(\theta_1)\cap N_2(\theta_2)\neq 0$

任取$N_1(\theta_1)\cap N_2(\theta_2)$中非零元y，有$y(\theta_1-\theta_2)=y\theta_1-y\theta_2=0$. 即$\theta_1-\theta_2$不是M的一个同构。于是$\theta_1-\theta_2$是无势的，否则与上题结论矛盾. 即$\theta_1-\theta_2\in R$. 其次对E中任一元$\beta$，及R中任一元$\theta$，显然$\beta\theta$仍是M的一个A—自同态.因$\theta$不是同构，故$\beta\theta$也不是同构.于是$\beta\theta$是无势的. 即$\beta\theta\in R$. 同样地有$\theta\beta\in R$. 所以R是E的一个理想。

如果$\alpha\in E$是一个左零因子.即存在$0\neq\beta\in E$，使$\alpha\beta=0$. 显然α不是M的一个同构,否则α有逆α^{-1},则$\alpha^{-1}(\alpha\beta)=(\alpha^{-1}\alpha)\beta=\beta=0$. 与$\beta\neq 0$矛盾。同上面一样，此时$\alpha$是无势的. 即$\alpha\in R$.

习 题 67

1. 如果B的所有相伴素理想是极大的。求证：B分解为带有不同相伴素理想的准素理想的无赘交只有一种分解法

〔证明〕设$B=Q_1\cap Q_2\cap\cdots Q_s=Q_1'\cap Q_2'\cap\cdots Q_r'$

p_i是Q_i的相伴素理想，$i=1,2\cdots s$.

p_i'是Q_i'的相伴素理想，$i=1,2\cdots r$.

且当$i\neq j$时，$p_i\neq p_j, p_i'\neq p_j'$. B是准素理$Q_1,Q_2\cdots Q_s$的无赘交，也是准素理想$Q_1',Q_2'\cdots Q_r'$的无赘交，且$p_i$与$p_i'$都是环A中的极大理想。

由第一唯一性定理可知$r=s$，且将Q_i'的次序适当排列

后，可得$p_i = p_i'$，$i = 1, 2 \cdots s$。

今证$Q_i = Q_i'$，$i = 1, 2 \cdots s$。因为所有的p_j，$j = 1, 2 \cdots s$都是极大的。所以p_i不包含B中其余的相伴素理想，即Q_i是B的孤立准素理想。同理，Q_i'也是B的孤立准素理想，且$p_i = p_i'$。由第二唯一性定理可知$Q_i = Q_i'$（$i = 1, 2 \cdots s$），从而证得满足题设的条件的分解法是唯一的。

2. 求证：诺德环里理想的根集是相伴素理想的交。

〔证明〕设B是诺德环里的理想，且$B = Q_1 \cap Q_2 \cap \cdots \cap Q_r$是B分解为准素理想的无赘交的分解式，则$R(Q_i)$，$i = 1, 2 \cdots r$是B的相伴素理想。由本书习题65第3题可得$R(B) = R(Q_1 \cap Q_2 \cap \cdots \cap Q_r) = R(Q_1) \cap R(Q_2) \cap \cdots \cap R(Q_r)$

3. 求证：根集是一个素理想必须而且只须给定的理想只有一个孤立准素理想。

〔证〕：设给定的理想为B，且$B = Q_1 \cap Q_2 \cap \cdots \cap Q_r$是B分解为准素理想的无赘交，这些准素理想的相伴素理想互不相同。令$s_i = R(Q_i)$（$i = 1, 2, \cdots r$）

依上题有$R(B) = R(Q_1) \cap R(Q_2) \cap \cdots \cap R(Q_r) = p_1 \cap p_2 \cap \cdots \cap p_r$。此时在$p_1, p_2, \cdots, p_r$中存在有一个极小素理想，即它不包含组内其他任何一个素理想的素理想。不妨记这个极小素理想为p_1，亦即Q_1是B的一个孤立准素理想。于是

$$R(B) = P_1 \cap (p_2 \cap p_3 \cdots \cap p_r).$$

显然每个素理想都是不可约的。因为如果一个素理想p可以表示为　$p = A \cap B$，且$A \supset p$，$B \supset p$，则有

$$AB \equiv 0 \ (\mathrm{mod}\, A \cap B) \equiv 0 \ (\mathrm{mod}\, p) \text{而} A \not\equiv 0 \ (\mathrm{mod}\, p),$$

$B \not\equiv 0 \ (\mathrm{mod}\, p)$.

这与p是素理想的性质矛盾。（习题65第2题），

因而若R(B)是素理想，则R(B)是不可约的。

如果B还有另一个孤立准素理想，不妨设为Q_2，则R(B) $=p_1\cap p_2\cap(p_3\cap\cdots\cap p_r)$，其中 $p_1\supset R(B)$，$p_2\supset R(B)$。且$p_1\cap p_2\neq p_i$（$i=1,2$）

这与R(B)是不可约矛盾.

反之，若B只有一个孤立准素理想，不妨设为Q_1，R(B) $=p_1\cap p_2\cap\cdots\cap p_r$。由$Q_2$不是B的孤立准素理想．所以$p_2$必含有其余某个$p_i$，则$p_2$可从$p_1\cap p_2\cap\cdots\cap p_r$中去掉。

同理$p_3,\cdots p_r$都可从中去掉，得$R(B)=p_1$。即R(B)是素理想。

4．如果B是一个理想，则$\bigcap\limits_i B^i$（$i=1,2,3,\cdots$）叫做B的ω一幂，记作Bω．令B是诺德环里一个理想，并令BωB $=Q_1\cap Q_2\cap\cdots\cap Q_n$是准素理想的无赘交。求证 $Q_j\supseteq B\omega$（$j=1,2,\cdots,n$），由此求证：$B\omega B=B\omega$。

〔证〕：显然$B\omega B\subseteq Q_j$（$j=1,2,\cdots,n$）

若$B\subseteq Q_j$．则$B\omega\subseteq Q_j$。

若$B\not\subseteq Q_j$．则存在$b\in B$，而$b\notin Q_j$．于是对B^w中任意元c，有$cb\in Q_j$．因Q_j是准素理想，所以$c\in R(Q_j)$．则$B\omega\subseteq R(Q_j)=p_j$，由于B是诺德环里的理想。满足因子链条件。则存在正整数r，使$p_j^r\subseteq Q_j$。

于是$(B\omega)^r\subseteq p_j^r\subseteq Q_j$．而$(B\omega)^r=B\omega$。

所以　　$B\omega\subseteq Q_j$（$j=1,2,\cdots,n$）。

今证$B\omega B=B\omega$。

显然$B\omega B\subseteq B\omega$．又$B\omega\subseteq Q_j$（$j=1,2,\cdots n$）．

于是$B\omega\subseteq Q_1\cap Q_2\cap\cdots\cap Q_n=B\omega B$．故$B\omega B=B\omega$。

习 题 68

1．如果$m=-3$，求证G是欧儿里的整区。

〔证明〕首先验证$G=\{\alpha+\beta\sqrt{-3}\mid\alpha,\ \beta$都是整数或都是奇数的$\frac{1}{2}\}$是复数域的子环。设a，$b\in G$即$a=\alpha_1+\beta_2\sqrt{-3}$，$b=\alpha_2+\beta_2\sqrt{-3}$（$\alpha_1,\alpha_2,\beta_1,\beta_2$都是整数或都是奇数的$\frac{1}{2}$）。

显然$a-b=(\alpha_1-\alpha_2)+(\beta_1-\beta_2)\sqrt{-3}\in G$

而$a\cdot b=(\alpha_1+\beta_1\sqrt{-3})(\alpha_2+\beta_2\sqrt{-3})=(\alpha_1\alpha_2-3\beta_1\beta_2)+(\alpha_1\beta_2+\alpha_2\beta_1)\sqrt{-3}\overset{记}{=}\alpha_3+\beta_3\sqrt{-3}$

分别令$\alpha_1,\alpha_2,\beta_1,\beta_2$都是整数或都是奇数的$\frac{1}{2}$或者$\alpha_1$，$\beta_1$与$\alpha_2,\beta_2$中一组都是整数另组都是奇数的$\frac{1}{2}$，直接验证易知$\alpha_3$与$\beta_3$或者同是整数或者同是奇数的$\frac{1}{2}$。故$ab\in G$。

其次，因为复数域满足交换律和消去律．且$1+0\sqrt{-3}\in G$是G中的恒等元素，故G是带恒等元素的可换整区。

最后，定义$\delta(m+n\sqrt{-3})=m^2+3n^2$．对于如上面取定的任意的$a,b\in G\ (b\neq 0)$

$$\frac{a}{b}=\frac{\alpha_1+\beta_1\sqrt{-3}}{\alpha_2+\beta_2\sqrt{-3}}\overset{记}{=}\alpha'+\beta'\sqrt{-3}.$$ α',β'为有理数。

必可找到都是整数或者都是奇数的½的两个数u，v使得

$|\alpha'-u|\leqslant\frac{1}{2}$．$|\beta'-v|\leqslant\frac{1}{4}$

（具体方法先找到满足条件的v后再确定u）

于是$a=b(\alpha'+\beta'\sqrt{-3})=b(u+v\sqrt{-3})+b[(\alpha'-u)+(\beta'-v)\sqrt{-3}]\overset{记}{=}bq+r$

因为a，$b(u+v\sqrt{-3})\in G$

所以$r=b[(\alpha'-u)+(\beta'-v)\sqrt{-3}]=a-b(u+v\sqrt{-3})\in G$

且$\delta(r)=\delta(r)\bar{\delta}[(\alpha'-n)+(\beta'-v)\sqrt{-3}]=\delta(b)[(\alpha'-u)^2+3(\beta'-v)^2]\leqslant\delta(b)(\frac{1}{4}+\frac{3}{16})=\delta(b)\frac{7}{16}<\delta(b)$因此G是欧几里的整区。

2.求证：m只有五个负值，即$m=-1,-2,-3,-7,-11$，使G关于函数$\delta(\alpha)=|N(\alpha)|$成欧几里得整区。

证：G关于函数$\delta(\alpha)=|N(\alpha)|$成欧几里得整区，即对G中任意二个数$\xi$，$\eta$（$\eta\neq0$），恒有二整数K与$\lambda$存在，使

$$\xi=K\eta+\lambda,\quad |N(\lambda)|<|N(\eta)|$$

它等价于对G中任意一个数ξ，必有一整数K存在，使

$$|N(\xi-K)|<1 \qquad (*)$$

1）若$m\equiv2$或$3\pmod 4$，取$\xi=r+s\sqrt{m}$，$K=x+y\sqrt{m}$，则（*）变为对任意一对有理数r，s，有有理整数x，y使

$$|(r-x)^2-m(s-y)^2|<1$$

若取$r=s=\frac{1}{2}$，则上式可化成$\frac{1}{4}+|m|\frac{1}{4}<1$，即$|m|<3$

故若$|m|\geqslant3$，则$R_0(\sqrt{m})$，（$m<0$）非欧几里得整区。

因对任何有理数r，s恒有有理整数x，y使

$$|r-x|\leqslant\frac{1}{2},\quad |s-y|\leqslant\frac{1}{2}$$

故对$m=-1,-2$时

$$|(r-x)^2-m(s-y)^2|\leqslant\frac{1}{4}+|m|\frac{1}{4}<1$$

恒成立，所以m＝－1，－2时，G是欧几里得整区。

2）若$m\equiv1\pmod 4$，取

$$\xi=r+s\sqrt{m},\quad K=x+\frac{1}{2}y(1+\sqrt{m})$$

故得：$|(r-x-\frac{1}{2}y)^2-m(s-\frac{1}{2}y)^2|<1$

取$r=s=\frac{1}{4}$，则得

$$\frac{1}{16}+\frac{1}{16}|m|<1,\text{ 即 }|m|<15。$$

故当$m\equiv1\pmod 4$时，只可能有三个欧几里得整区，即m＝－3，－7，－11。反之，因为对任何有理数r,s总有有理整数x,y，使

$$|2s-y|\leqslant\frac{1}{2},\quad |r-x-\frac{1}{2}y|\leqslant\frac{1}{2}$$

于是当m＝－3，－7，－11时

$$|(r-x-\frac{1}{2}y)^2-m(s-\frac{1}{2}y)^2|\leqslant\frac{1}{4}+|m|\frac{1}{16}\leqslant\frac{15}{16}<1$$

故m＝－3，－7，－11时确是欧几里得整区。

第七章　格

习　题　69

1.求证：由阶数为素数幂的一个循环群的子群构成的半序集合是一个链。

证：设循环群$G=\{a\mid a^{p^\alpha}=1,\ p\text{是素数}\}$，那末G的子群的阶是$p^\alpha$的约数，设为$p^\beta$（$0\leqslant\beta\leqslant\alpha$），而关系“$\geqslant$”表示“$\supseteq$”（包含的意思），显然满足$p_1,p_2$两个关系式。

其次：设H_1，H_2为G的任意两个子群，即$H_1=\{ap^{\alpha_1}\}$，$H_2=\{ap^{\alpha_2}\}$，而α_1，α_2为整数，则或者$\alpha_1\geqslant\alpha_2$，或者$\alpha_1\geqslant\alpha_2$，故必有$H_1\geqslant H_2$或者$H_1\geqslant H_2$，故这一半序集是一个链。

2．令s是在区间$0\leqslant x\leqslant 1$上连续的所有函数的集合，并且定义$f\geqslant g$，必须而且只须对于闭区间内所有x，$f(x)\geqslant g(x)$，求证：关系$\geqslant$是s的一个半序关系。

证：p_1：若$f\geqslant g$，$g\geqslant f$，显然可推出$f=g$（$\because f(x)=g(x)$，$0\leqslant x\leqslant 1$）

p_2：若$f\geqslant g$，$g\geqslant h$可推出$f\geqslant h$

$\because f(x)-g(x)\geqslant 0$，$g(x)-h(x)\geqslant 0$，$0\leqslant x\leqslant 1$

$\therefore f(x)-g(x)+g(x)-h(x)=f(x)-h(x)\geqslant 0$，$0\leqslant x\leqslant 1$

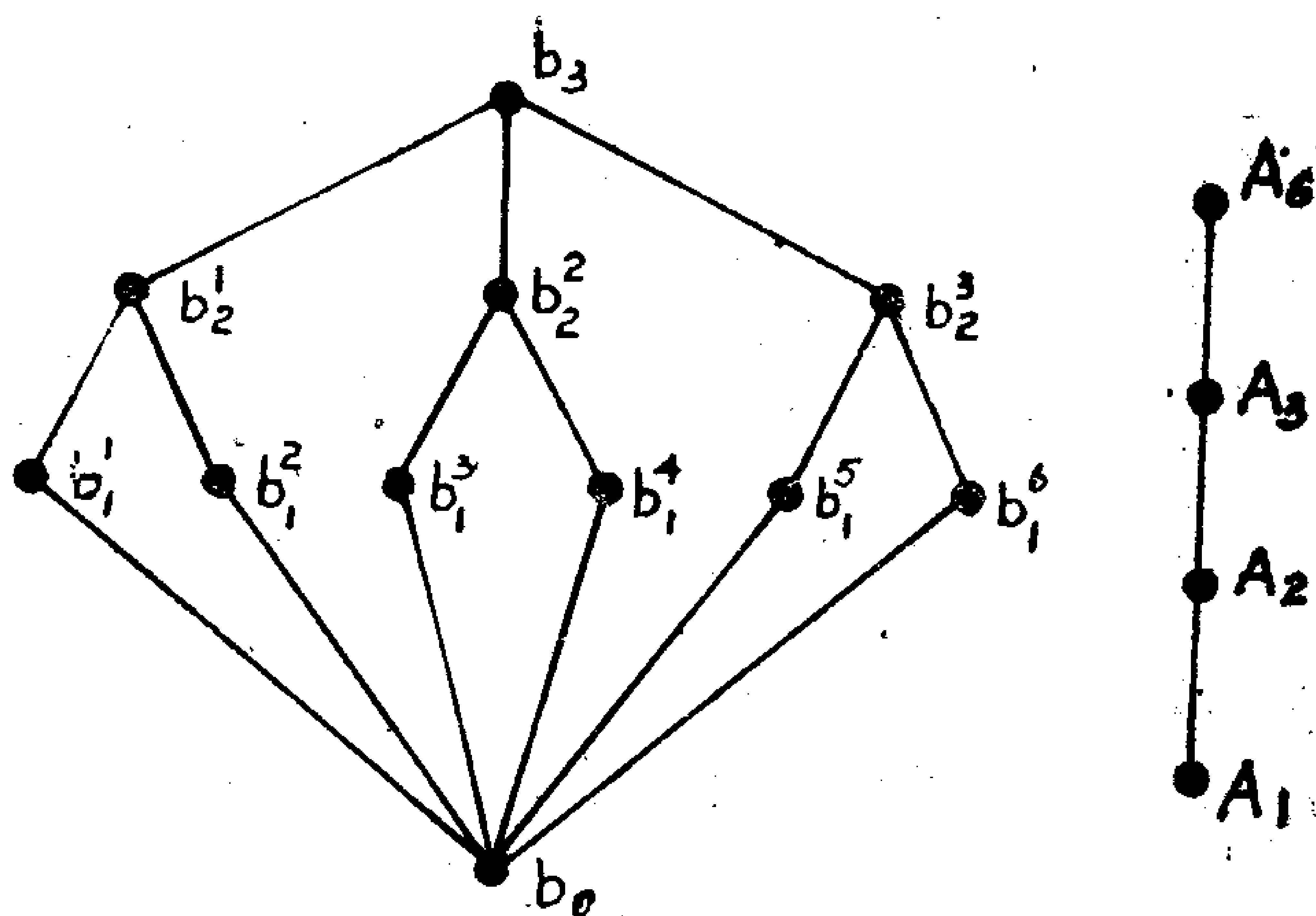
且s中任意两元素f_1，f_2可以比较其是$f_1\geqslant f_2$与否，故关系$\geqslant$是s的一个半序关系。

3．求下列半序集合的图解：由含有三个元素的集合的子集合构成的集合．6阶循环群的子群构成的集合；s_3的子群构成的集合。

解：（1）以b_i表示含有i个元素的集合，又以$b^1{}_i,b^2{}_i$表示同是含有i个元素的不同集合，显然b_3及b_0只有一个，结果见下页左图。

（2）以A_i表示阶为i的循环群。显然A_6只有一个6阶循环群。

$A_6=\{a\mid a^6=1\}$，$A_3=\{a^2\}$，$A_2=\{a^3\}$，$A_1=\{a^6\}=\{1\}$，见下页右图。

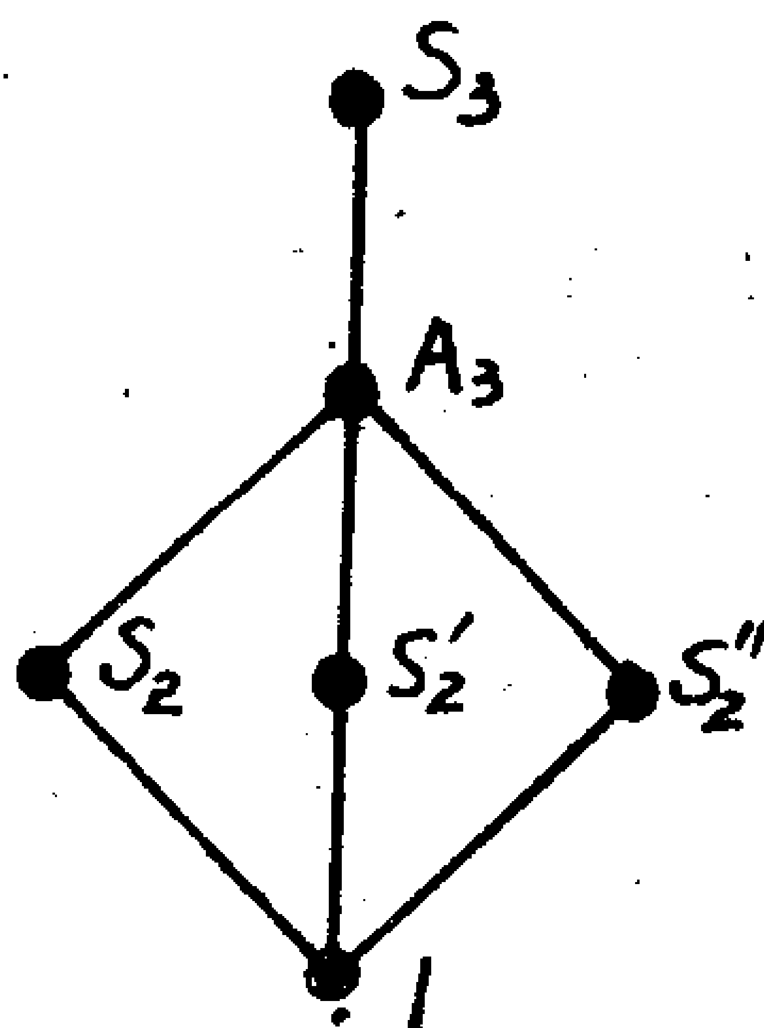


(3) S_3的子群构成的集合。　　　∵S_3是三次对称群

记S_3 = {(1), (12), (13), (23), (123), (132)}

A_3 = {(1), (123), (132)}

S_2 = {(1), (12)}, S_2' = {(1), (13)}, S_2'' = {(1), (23)}, 1 = {(1)}.



习　题　70

1. 求证：任一个群的不变子群（关于任一个算子集合M的）M—子群的集合都是这个群的子群构成的格的子格。

证：设G是任意一个群，则$A\cup B=\{A, B\}$，而$A\cap B$为子群A与B的共同部分。

（1）若A，B是G的不变子群，则$A\cap B$也是G的不变子群

∵若$c\in A\cap B$，即$c\in A$，$c\in B$则对于G中任一元g，$g^{-1}cg\in A$，$g^{-1}cg\in B$因而$g^{-1}cg\in A\cap B$，又∵A，B是不变子群，故$A\cap B$是G的不变子群。

其次，$A\cup B=[A, B]$也是G的不变子群

∵$A\cup B=(a_1a_2\cdots a_n \mid a_i\in A$ 或 $a_i\in B$，$i=1 2\cdots n$，n为任意整数）

设$a_1a_2\cdots a_u\in A\cup B$，g是G中任一元。

∵A，B为不变子群，所以$g^{-1}a_ig\in A$，或B（视$a_i\in A$或$a_i\in B$），显然$g^{-1}a_1gg^{-1}a_2gg^{-1}a_3\cdots g^{-1}a_ug=g^{-1}a_1a_2\cdots a_ug\in A\cup B$则$A\cup B$也是G的不变子群，故任一个群G的不变子群的集合都是这个群G的子群构成的格的子格。

（2）设A，B是G的M—子群，则$A\cap B$也是G的M—子群（∵若$a\in A\cap B$，即对M中任一元m，$ma\in A$，$ma\in B$则$ma\in A\cap B$）。

其次，$A\cup B$也是M—子群。

∵对$A\cup B$中任一元$a_1a_2\cdots a_u$，$a_i\in A$或B，有

$m(a_1a_2\cdots a_u)=(ma_1)(ma_2)\cdots(ma_u)\in A\cup B$，故G中所有M—子群的集合都是G的子群构成的格的子格。

2. 令S表示习题69的第2题里的半序集合，求恰当地定

义$f\cup g$及$f\cap g$，并证：S对于这些合成及给定的半序关系构成一个格，S成一个完全格吗？

证：先定义$\cup$和$\cap$

(1)若$f\geqslant g$则定义$f\cup g=g$，$f\cap g=g$

(2)若$f\ngeqslant g$则定义$f\cup g=h$，$h(x)$是这样的连续函数，$h(x_i)=\max[f(x_i),\ g(x_i)]$，$0\leqslant x_i\leqslant 1$，而$f\cap g=k$，$k(x_i)=\min[f(x_i),\ g(x_i)]$，$0\leqslant x_i\leqslant 1$。

对上面所定义的$\cup$和$\cap$，在S中任二元，显然有一最小上界和一最大下界，故S构成格，（∵若$f\cup g=h$则S中任一元w，满足$w\geqslant f$，$w\geqslant g$可推出$w\geqslant h$，同理$f\cap g=k$是最大的下界）

其次：如此所定义的格S是一个完全格。

∵若$\{f_\alpha\}\subseteq S$，而每一个$f_\alpha(x_i)<\infty$，$0\leqslant x_i\leqslant 1$，故$\max[f_1(x_i)\cdots,\ f_\alpha(x_i),\ \cdots]$存在，又每一个$f_\alpha(x_i)>-\infty$

$0\leqslant x_i\leqslant 1$，故$\min[f_1(x_i),\ \cdots,\ f_\alpha(x_i),\ \cdots]$存在，所以S中任一个子集必有一个最小上界和一个最大下界

3.求证：任一个完全格有一个零元素及一个全元素。

证：设G是一个完全格，那末G当然可视为它本身的一个子集，依定义，G有一个最小上界和一个最大下界，此即为G的全元素和零元素。

4.如果带有一个全元素的一个半序集合里，每个非空子集合有一个g.l.b求证：这个半序集合是一个完全格。

证：设S是带有一个全元素的一个半序集合，我们先证明S是一个格。

∵S里的任一元素a，有$1\geqslant a$，又S里每个非空子集合

有一个g.1.b，因而子集合里每个元素有g.1.b，从而说明S里任意两个元素都有一个最小上界及一个最大下界，所以S是一个格。

其次，若A为S中任一非空子集合，如果A包含全元素1，则1即为A的最小上界。

若A不包含1，但由于A中的每一个元素都有上界，因而A必有最小上界，再由已知条件及定义知S是一个完全格。

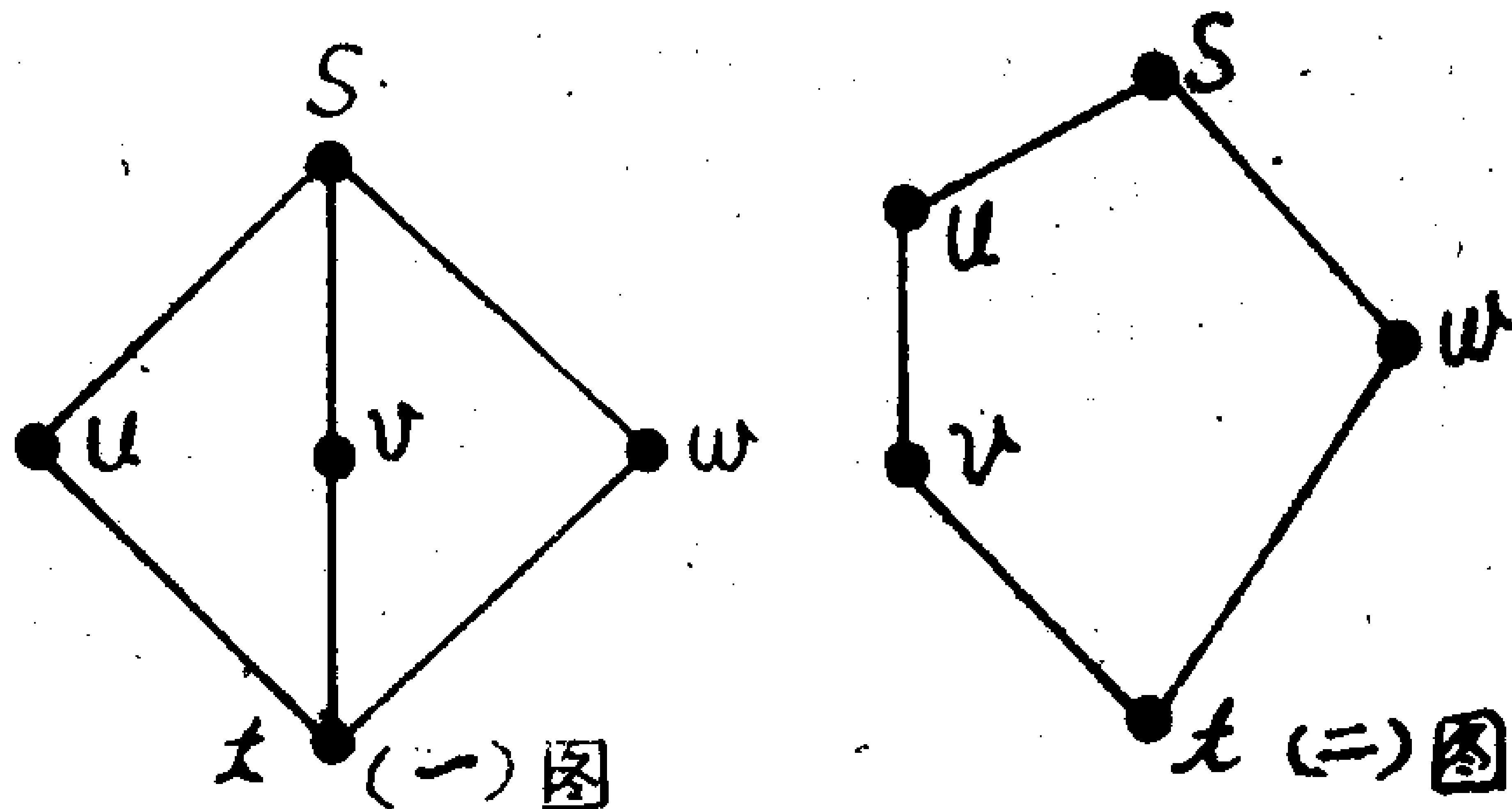
习　题　71

1.如果一个格不是分配的，求证一个5阶子格，其图解是§1里第1图或第2图；并证明：一个非模格含有一个子格，其图解是§1里第1图。

证：先证第二部分，为了达到这个目的，我们先说明格L是模格的充要条件为L不含有适合条件

$u \geqslant v$且$u \cup w = v \cup w$，$u \cap w = v \cap w$的三个元素u,v,w

并设$s = u \cup w (= v \cup w)$，$t = u \cap w (= v \cap w)$，由此可知，L是模格的充要条件为：L不含如图(一)、(二)那样的由五个元作成的子格。



(一)图　　(二)图

下面就来证明：假设有适合（1）的三个元，则因$u \geqslant v$，且$u \cap (v \cup w) = u \cap (u \cup w) = u \geqslant v = v \cup (v \cap w) = v \cup (u \cup w)$，故由定义可知，L不是模格。

反之，若L不是模格，则有适合

$a \geqslant c$，$a \cap (c \cup b) > c \cup (a \cap b)$的a,b,c

若令$u = a \cap (c \cup b)$，$v = c \cup (a \cap b)$，则

$u \cap b \geqslant v \cap b \geqslant (a \cap b) \cap b = a \cap b = a \cap (c \cup b) \cap b = u \cap b$

$\therefore n \cap b = v \cap b$，再由对偶性得$u \cup b = v \cup b$因此，若设$w = b$，则得（1），其图如(一)。

其次证第一部分：如果格L不是分配的，则格L也不满足L_5，故L也不是模格，再由上面已证过的结论得知L有一个5阶子格，其图解为图(一)或(二)。

2.求证：A_4的子群构成的格不是模格

证：从习题14第1题（2）可知

$A_4 = \{ \alpha_1, \alpha_3, \alpha_5, \alpha_8, \alpha_{10}, \alpha_{12}, \alpha_{13}, \alpha_{16}$
$\alpha_{17}, \alpha_{20}, \alpha_{21}, \alpha_{24} \} = \{ (1), (234), (243),$
$(12)(34), (123), (124), (132), (134), (13)(24),$
$(142), (14), (14)(23) \}$

再从A_4中，可知它的子群共有10个，即

A_4

$L_4 = \{ (1), (12)(34), (13)(24), (14)(23) \}$

$L_3 = \{ (1), (234), (243) \}$

$L_3' = \{ (1), (123), (132) \}$

$L_3'' = \{ (1), (124), (142) \}$

$L_3''' = \{ (1), (134), (143) \}$

$L_2 = \{ (1), (12)(34) \}$

$L_2' = \{(1), (13)(24)\}$

$L_2'' = \{(1), (14), (23)\}$

$L_1 = \{(1)\}$

$\because L_4 > L_2$, $L_4 \cap (L_2 \cup L_3) = L_4 \cap A_4 = L_4$

$L_2 \cup (L_4 \cap L_3) = L_2 \cup L_1 = L_2$

$\therefore L_4 \cap (L_2 \cup L_3) \neq L_2 \cup (L_4 \cap L_3)$

故A_4的子群构成的格不是模格。

3.如果G是一个群，由两个元素a及b生成，而a及b适合$a^{p^m} = 1$，$b^{p^r} = 1$，$b^{-1}ab = a^n$，这里$n^{p^r} \equiv 1 \pmod{p^m}$求证：G的任意两个子群可交换，应用这结果求证：G的子群构成的格是模格。

证：（1）∵G是一个群，且它是由a及b生成的，故在G中，它的子群有G=〔ab〕本身还有〔1〕、〔a〕、〔b〕以及〔a〕中子群及〔b〕中子群。但在〔a〕中的任意两个子群显然是可以交换的，同样〔b〕中的任意两个子群也是可以交换的。再由条件$b^{-1}ab = a^n$，$p^m \mid r^{p^r} - 1$可知〔a〕是不变子群，故有〔a〕〔b〕=〔b〕〔a〕≤〔a〕，∴G中任意两个子群都可以交换。

（2）设g_1，g_2，g_3是G的任意三个可交换的子群，其中不妨设$g_1 \geqslant g_2$，先考虑$g_1 \cap (g_2 \cup g_3)$。而$g_2 \cup g_3$表示g_1，g_2的l.u.b，故$g_2 \cap g_3$是由g_2，g_3生成的子群，且$g_2 \cup g_3 = g_2g_3 = g_3g_2$，于是若$m \in g_1 \cap (g_2 \cup g_3)$则$m = h_1 \in g_1$且$m = h_2h_3$这里$h_2 \in g_2$，$h_3 \in g_3$由$h_1 = h_2h_3$得$h_2^{-1}h_1 = h_3$，∵$g_1 \geqslant g_2$，故这个等式的左端表示$g_1$的一元素，于是$h_3 \in g_1$，从而$h_3 \in g_1 \cap g_3$，∴$g_1 \cap (g_2 \cup g_3) \leqslant g_2 \cup (g_1 \cap g_3)$，又∵倒转不等式是一般格论的性质。

$\therefore g_1 \cap (g_2 \cup g_3) \geqslant g_2 \cup (g_1 \cap g_3)$

故有$g_1 \cap (g_2 \cup g_3) = g_2 \cup (g_1 \cap g_3)$

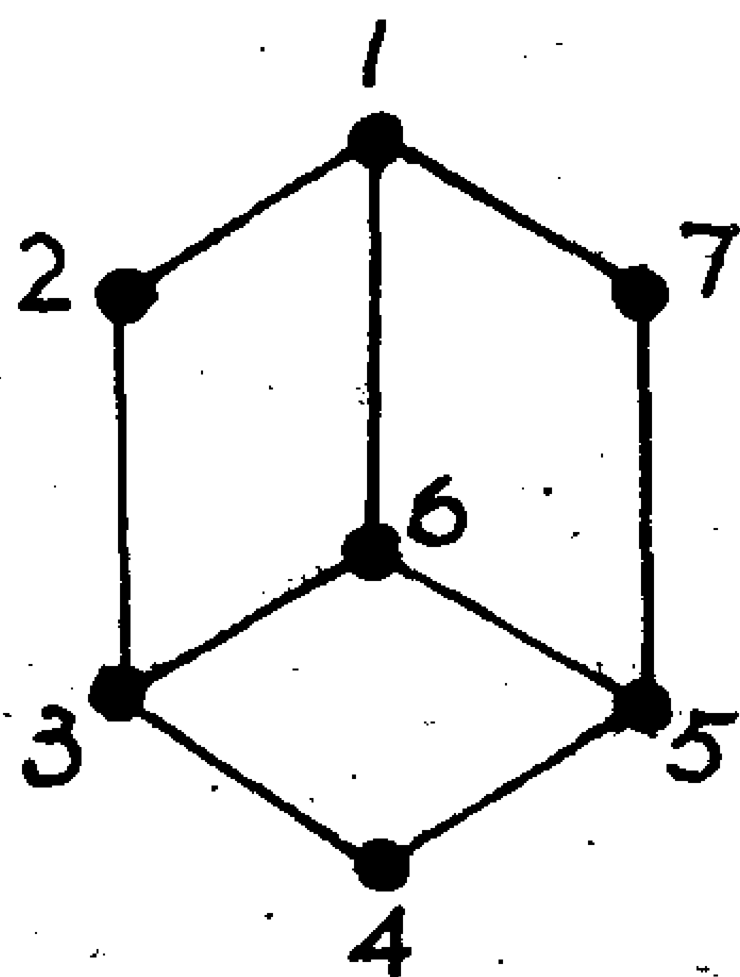
∴G的子群构成的格是模格。

4.如果在一个模格L里，a复盖$a \cap b$，求证：$a \cup b$复盖b，具有这个性质的格叫做半模格。验证：具有下面图解的格是半模格，但不是模格。

证：设a复盖$a \cap b$，此时，只有两种情况

(i)$a > b$，且a复盖b，则$a \cup b = a$复盖b

(ii)a与b，不能互相比较，这时若$a \cup b$不能复盖b，即存在一元素c，使$a \cup b > c > b$，且$c \neq a$，这时就有适合$c > b$且$c \cup a = b \cup a (= a \cup b)$ $c \cup (b \cup a) = c \cap (c \cup a) = c >$ $b = b \cup (a \cap b) = b \cup (c \cap a)$故L不是模格，与已知矛盾，因此$a \cup b$复盖b。



其次，验证具有上面图解的格是半模格，但不是模格。

若要证它为半模格，只须证明下面几种情况(因为a,b互相复盖者不必证明，那是显然成立的)

(i)$a = 2$，$b = 6$，则$a \cap b = 3$被a复盖，而$a \cup b = 1$复盖b。

(ii)$a=3$，$b=5$，也显然成立。

满足a复盖$a\cap b$者（除a,b互相复盖外）只有以上两种，故此格是半模格。

下证它是非模格。∵ 当$a=2$，$b=3$，$c=7$时，满足$a\geqslant b$而$a\cap(b\cup c)=2\cap 1=2$

$b\cup(a\cap c)=3\cup 4=3$

$2\neq 3$ 故非模格

习　题　72

1.设A是格L的一个子集合，如果(1)$a,b\in A$可推得$a\cap b\in A$，并且(2)$a\in A$及$x\in L$可推得$a\cup x\in A$，则说A是一个理想，如果对于固定的$a\in L$，A由能使$x\geqslant a$的所有$x\in L$构成，则A叫做一个主理想，记作(a)。求证：L适合降链条件必须而且只须L的每个理想是主理想。

证：必要性：设L是格，且适合降链条件，今设A是格L的子集合，它是$A=\{x\mid x\geqslant a\in L$，a是固定$\}$

若$b,c\in A$，且$b>c$，则由题设知$b=b_1>b_2>\cdots>b_{n+1}=c$，其中每个$b_i$是$b_{i+1}$的一个复盖，再由格的定义知它们必满足半序定义中的$p_2$，故$b>c$，∴$b\cap c=c\in A$。

其次，若$b\in A$，$x\in L$，由格的定义知$b\cup x$存在，再由上面给出A的条件知$b\cup x\in A$，∴A是一个主理想。

充分性：设L的每个理想是主理想，则由定义知，若a，$b\in A$，当然$b\in L$，即有$a\cap b\in A$，$a\cup b\in A$，说明A的任意两个元素的l.u.b及g.l.b存在，且若$a>b$，则有

$(a\cup b)>a>b>(a\cap b)\cdots(1)$

若$(a\cup b)$复盖a，a复盖b，b复盖$(a\cap b)$则(1)已是合成链，

否则，我们总可以得到$(a\cup b)=a_1>a_2>\cdots>a>a_1'>\cdots>a_s'>b>b_1>\cdots>b_r=(a\cap b)$为止，其中后一个总是被前一个复盖。这样已是合成链。若$a\not> b$，但有$a\cup b>a>a\cap b$ …（2），$a\cup b>b>a\cap b$ …（3）。若（2）、（3）两式的前项复盖后一个，则（2）、（3）也是合成链，否则仿上也可以得到合成链。

习　题　73

1. 如果a_1，a_2，…，a_r是一个无关集合，求证：任一子集合是无关的；并证明：元素

$b_1=a_1\cup\cdots\cup a_{r_1}$，$b_2=a_{r_1+1}\cup\cdots\cup a_{r_2}$，$b_k=a_{r_{k-1}+1}\cup\cdots\cup a_{r_k}$是无关元素，这里$r_1<r_2<\cdots<r_k=n$。

证：设$i_1\cdots i_s\cdots i_n$是1，2，…，n的任一种排列。

$\{a_{i_1}\cdots a_{i_s}\}$是$\{a_1\cdots a_u\}$的任一个子集合，$i_s\leqslant n$

因为$a_{ij}\cap(a_{i_1}\cup a_{i_2}\cup\cdots\cup a_{i_{t-1}}\cup a_{i_{t+1}}\cup\cdots\cup a_{i_s}\leqslant$

$a_{i_t}\cap(a_{i_1}\cup a_{i_2}\cup\cdots\cup a_{i_{t-1}}\cup a_{i_{t+1}}\cup\cdots\cup a_{i_{s+1}}\cup\cdots\cup a_{i_n})=0$ $(i_t=i_1,\ \cdots,\ i_s)$

故$\{a_{i_1}\cdots a_{i_s}\}$是无关的。

其次：证b_1，…，b_k是无关元素

∵a_1，a_2，…，a_r是一个无关集合，由定理9的证明可知$(a_1\cup\cdots\cup a_s)\cap(a_{s+1}\cup\cdots\cup a_n)=0$

故$b_i\cap(b_1\cup\cdots\cup b_{i-1}\cup b_{i+1}\cup\cdots\cup b_k)=0$，$i=1$，…，k，故$b_1$，…，$b_k$是无关元素。

2. 令a_1，…，a_r是无关元素的一个集合，且有$a_1\cup a_2\cup\cdots\cup a_n=1$，定义$b_i=a_1\cup\cdots\cup a_{i-1}\cup a_{i+1}\cup\cdots\cup a_n$…（1）

求证对偶关系：

$$b_i \cup (b_1 \cap \cdots \cap b_{i-1} \cap b_{i+1} \cap \cdots \cap b_n) = 1$$

$$b_1 \cap b_2 \cap \cdots \cap b_n = 0$$

$$a_i = b_1 \cap \cdots \cap b_{i-1} \cap b_{i+1} \cap \cdots \cap b_n$$

证：在(1)式中，b_i这个元素不包含a_i，而其余$n-1$个a_j都包含在b_i内，又从定理9可知：

$$(a_1 \cup \cdots \cup a_r \cup a_{r+1} \cup \cdots \cup a_s) \cap (a_1 \cup \cdots \cup a_r \cup a_{s+1} \cup \cup a_t) = a_1 \cup \cdots \cup a_r$$

故$b_1 \cap b_2 = a_3 \cup \cdots \cup a_n \rightarrow b_1 \cap b_2 \cap \cdots \cap b_{i-1} \cap b_{i+1} \cap \cdots \cap b_n = a_i \cdots (1)$

则$b_i \cap (b_1 \cup \cdots \cup b_{i-1} \cup b_{i+1} \cup \cdots \cup b_n) = (a_1 \cup \cdots \cup a_{i-1} \cup a_{i+1} \cdots \cup a_n) \cup a_i = a_1 \cup a_2 \cup \cdots \cup a_{i-1} \cup a_i \cup a_{i+1} \cup \cdots \cup a_n = 1$

其次：$b_1 \cap b_2 \cap \cdots \cap b_n = (b_1 \cap b_2 \cap \cdots \cap b_{n-1}) \cap b_n$
$= a_n \cap (a_1 \cup a_2 \cup \cdots \cup a_{n-1}) = 0$

最后：由(1)式即知$a_i = b_1 \cap b_2 \cap \cdots \cap b_{i-1} \cap b_{i+1} \cap \cdots \cap b_n$

3.如果元素a_1，a_2，…，a_n是无关的，并且$(a_1 \cup \cdots \cup a_n) \cap a_{n+1} = 0$

(1)求证：元素a_1，a_2，…，a_n，a_{n+1}是无关的；

(2)求证：集合a_1，a_2，…，a_n是无关的必须而且只须$(a_1 \cup \cdots \cup a_i) \cap a_{i+1} = 0$ ($i = 1, 2, \cdots, n-1$)

证(1)∵a_1，a_2，…，a_n是无关的

$$\therefore a_i \cap (a_1 \cup \cdots \cup a_{i-1} \cup a_{i+1} \cup \cdots \cup a_n) = 0 \cdots (1)$$

(1)式说明a_i与a_1，…，a_{i-1}，a_{i+1}，…，a_n的交都是零。

同样由$(a_1 \cup \cdots \cup a_n) \cap a_{n+1} = 0$，说明$a_{n+1}$与$a_1$，…，$a_n$的交也都是零，因此$a_i$与$a_1$，…，$a_{i-1}$，$a_{i+1}$，…，$a_n$，

a_{n+1}的交皆为零。

故$a_i \cap (a_1 \cup \cdots \cup a_{i-1} \cup a_{i+1} \cup \cdots \cup a_n \cup a_{n+1}) = 0$ （$i = 1, n+1$）

由定义知a_1，…，a_n，a_{n+1}是无关的。

（2）假设a_1，…，a_n是无关的，由习题73第1题知它们任一个子集合是无关的，因而有

$$(a_1 \cup \cdots \cup a_i) \cap a_{i+1} = 0 \quad (i = 1, \cdots, n-1)$$

反之，若$(a_1 \cup \cdots \cup a_i) \cap a_{i+1} = 0$ （$i = 1, \cdots, n-1$）说明a_1，a_2，…，a_n中的任一个元素与其余的元素的交都为零，因而$a_i \cap (a_1 \cup \cdots \cup a_{i-1} \cup a_{i+1} \cup \cdots a_n) = 0$。由定义知$a_1$，$a_2$，…，$a_n$是无关的。

4. 如果L适合链条件，求证：元素a_1，a_2，…，a_n是无关的必须而且只须

$$L(a_1 \cup a_2 \cup \cdots \cup a_n) = L(a_1) + L(a_2) + \cdots + L(a_n)$$

证：∵L满足链条件，故L是有限长。

设a_1，a_2，…，a_n是无关的，由本节第1题知它的任一子集合也是无关的。

故由$a_1 \cap (a_2 \cup a_3 \cup \cdots \cup a_n) = 0$即$l[a_1 \cap (a_2 \cup \cdots \cup a_n)] = 0$

再由维数关系公式得$l(a_1 \cup \cdots \cup a_n) = l[a_1 \cup (a_2 \cup \cdots \cup a_n)]$

$$= l(a_1) + l(a_2 \cup \cdots \cup a_n)$$

同理，因a_2，a_3，…，a_n无关的，故$l(a_2 \cup \cdots \cup a_n) = l(a_2 \cup (a_3 \cup \cdots \cup a_n)) = l(a_2) + l(a_3 \cup \cdots \cup a_n)$，以此类推，即得$l(a_1 \cup \cdots \cup a_n) = l(a_1) + l(a_2) + \cdots + l(a_n)$

反之，若$l(a_1 \cup \cdots \cup a_n) = l(a_1) + l(a_2) + \cdots + l(a_n)$我们证明$a_1$，$a_2$，…，$a_n$是无关的。

由维数关系公式得知：$l(a_1 \cup a_2 \cup \cdots \cup a_n) = l(a_1) + l(a_2 \cup a_3 \cup \cdots \cup a_n) - l[a_1 \cap (a_2 \cup \cdots \cup a_n)] = l(a_1) + l(a_2) + l(a_3 \cup \cdots \cup a_n) - l[a_1 \cap (a_2 \cup \cdots \cup a_n)] - l[a_2 \cap (a_3 \cup \cdots \cup a_n)] = \cdots = l(a_1) + l(a_2) + \cdots + l(a_n) - l[a_1 \cap (a_2 \cup \cdots \cup a_n)] - l[a_2 \cap (a_3 \cup \cdots \cup a_n)] - \cdots - l(a_{n-1} \cap a_n)$

由于$l(a_1 \cup \cdots \cup a_n) = l(a_1) + l(a_2) + \cdots + l(a_n)$故得$l(a_1 \cap (a_2 \cup \cdots \cup a_n)) + l(a_2 \cap (a_3 \cup \cdots \cup a_n) + \cdots + l(a_{n-1} \cap a_n) = 0$ 又维数$l[a_i \cap (a_{i+1} \cup \cdots \cup a_n)] \geqslant 0$因此 要使上式成立，只有$l[a_i \cap (a_{i+1} \cup \cdots \cup a_n)] = 0$故$a_i \cap (a_{i+1} \cup \cdots \cup a_n) = 0$（$i = 1, 2, \cdots, n-1$），再由本节第3题知$a_1, a_2, \cdots, a_n$是无关的。

习　题　74

1.求证：对于一个有余模格，可从两个条链件中的任一个推得另一个。

证：设L是一个有余模格则L带有0及1。今设L适合降链条件，则L含有点。

（1）若1是0的复盖，即1是一个点，则命题成立。

（2）若1不是0的复盖，即1不是一个点，则可选$a_1 > 0$，使$1 = a > a_1 > 0$，若a_1不是0的复盖，可选a_2，使$1 = a >_1 a > a_2 > 0$，由假设L适合降链条件，因此，这方法进行有限次后，必将停止下来，而达到L里一点a_n复盖0，即

$$1 = a > a_1 > a_2 > \cdots > a_n > a_{n+1} = 0 \cdots (1)$$

由此可见，这是L的一个合成链，由于这个链的存在，就可以推得两个链条件，从而也可从两个链条件中的任一个

推得另一个。

这是因为若 $p_1 \in L$ 一点，令 p_1' 是 p_1 的一个余元素，若 $p_1' \neq 0$ 由（1）得一点 $p_2 \leqslant p_1'$，$\because p_1 \cap p_2 = 0$，故 $p_1 \cup p_2 > p_1$，又 $\because p_1 \cup p_2$ 有一余元素，若它 $\neq 0$，必有一点 p_3，于是 $(p_1 \cup p_2) \cap p_3 = 0$ 且 $p_1 \cup p_2 \cup p_3 > p_1 \cup p_2 > p_1$，连续进行下去，得 p_1，p_2，p_3，…由（1）可知，到S次后，就要终止，当这种情况出现时，可知 $p_1 \cup p_2 \cup \cdots \cup p_s$ 有 0 作为余元素，这意味着 $1 = p_1 \cup p_2 \cup \cdots \cup p_s$ 故 1 是有限个点的一个l.u.b，且我们所选的 p_i 是使 $(p_1 \cup p_2 \cup \cdots \cup p_i) \cap p_{i+1} = 0$ $(i = 1 \cdots S-1)$。

习　题　75

1.求证：任一个布尔代数关于两个合成 $a \oplus b = (a \cup b') \cap (a' \cup b)$，$a \odot b = a \cup b$ 定义一个环。求证：$a \oplus b = 1 + a + b$，$a \odot b = a + b + ab$ 这里 + 及 · 是按书中定义的合成。

证：（1）$\oplus$ 满足交换律

$\because a \oplus b = (a \cup b') \cap (a' \cup b) = [(a \cup b') \cap a'] \cup [(a \cup b') \cap b] = (a \cap a') \cup (b' \cap a') \cup (a \cap b) \cup (b' \cap b)$
$= (b' \cap a') \cup (a \cap b)$

$b \oplus a = (b \cup a') \cap (b' \cup a) = [(b \cup a) \cap b'] \cup [(b \cup a') \cap a] = (b \cap b') \cup (a' \cap b') \cup (b \cap a) \cup (a' \cap a)$
$= (a' \cap b') \cup (b \cap a) \therefore a \oplus b = b \oplus a$

（2）$\oplus$ 满足结合律

首先 $\because (a \oplus b)' = [(b' \cap a') \cup (a \cap b)]' = (b' \cap a')' \cap (a \cap b)' = (b \cup a) \cap (a' \cup b')$

同理 $(b \oplus c) = (b \cup c') \cap (b' \cup c)$

$(b\oplus c)' = (c\cup b)\cap(b'\cup c')$

$(a\oplus b)\oplus c = [(a\oplus b)\cup c']\cap[(a\oplus b)'\cup c] = \{[(a\cup b')\cap(a'\cup b)]\cup c'\}\cap\{[(b\cup a)\cap(a'\cup b')]\cup c\}$
$= (a\cup b'\cup c')\cap(a'\cap b\cap c')\cap(b\cap a\cap c)\cap(a'\cup b'\cup c)$

$a\oplus(b\oplus c) = [a\cup(b\oplus c')]\cap[a'\cup(b\oplus c)] = \{a\cup[(c\cup b)\cap(b'\cup c')]\}\cap\{a'\cup[(b\cup c')\cap(b'\cup c)]\}$
$= (a\cup c\cup b)\cap(a\cup b'\cup c')\cap(a'\cup b\cup c')\cap(a'\cup b'\cup c)$

$\therefore (a\oplus b)\oplus c = a\oplus(b\oplus c)$

(3)对每一个a，$a\oplus 1 = (a\cup 1')\cap(a'\cup 1)$
$= (a\cup 0)\cap(a'\cup 1) = a\cap 1 = a$

即1是$\oplus$的0元

(4)对每一个a，$a\oplus a = (a\cup a')\cap(a'\cup a) = 1\cap 1$
$= 1$　　即a的逆元是a

故布尔代数关于$\oplus$是一个交换群

(5)对$\odot$法显然是结合的，因为关系$\cup$是结合的，且$\odot$是可交换的。

(6)对$\oplus\odot$满足分配律

$\because c\odot(a\oplus b) = c\cup(a\oplus b) = c\cup[(a\cup b')\cap(a'\cup b)]$
$= (c\cup a\cup b')\cap(c\cup a'\cup b)$

而$(c\odot a)\oplus(c\odot b) = (c\cup a)\oplus(c\cup b) = [(c\cup a)\cup(c\cup b)']\cap[(c\cup a)'\cup(c\cup b)] = [(c\cup a)\cup(c'\cap b')]\cap[(c'\cap a')\cup(c\cup b)] = (c\cup a\cup c')\cap(c\cup a\cup b')\cap(c'\cup c\cup b)\cap(a'\cup c\cup b) = 1\cap(c\cup a\cup b')\cap 1\cap(a'\cup c\cup b) = (c\cup a\cup b')\cap$

$(a' \cup c \cup b)$

$\therefore c \odot (a \oplus b) = (c \odot a) \oplus (c \odot b)$

同理$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$

故布尔代数关于$\oplus$，$\odot$运算成环。

对于第二部分：

$\because 1 + a + b = (1 + a) + b = [(1 \cap a') \cup (1' \cap a)] + b = [(1 \cap a') \cup (0 \cap a)] + b = a' + b = (a' \cap b') \cup (a \cap b) = a \oplus b$

$a + b + ab = [(a + b) \cap (ab)'] \cup [(a + b)' \cap (ab)]$
$= [[(a \cap b') \cup (a' \cap b)] \cap (a \cap b)'] \cup [[(a \cap b') \cup (a' \cap b)]' \cap (a \cap b)] = \{[(a \cap b') \cup (a' \cap b)] \cap (a' \cup b')\} \cup \{[(a \cap b')' \cap (a' \cap b)]' \cap (a \cap b)\}$
$= \{[(a \cap b') \cup (a' \cap b)] \cap (a' \cup b') \cup (a \cup b')]$
$\cap (a \cap b)\}$利用可分配的及交的性质得
$= (a \cap b') \cup (a' \cap b) \cup (a \cap b)$

再利用可分配的及有余的性质得
$= [(b' \cup a' \cup a) \cap (b' \cup a' \cup b)] \cap [(a \cup b \cup a) \cap (a \cup b \cup b)] = (1 \cap 1) \cap (a \cap b) \cap (a \cup b)$
$= (a \cup b) = a \odot b$

故$a \oplus b = 1 + a + b$；$a \odot b = a + b + ab$

注：在上面计算中$(b' \cap a \cap b) = 0$　　$(a \cap b' \cap a') = 0$　　$(a' \cap a \cap b) = 0$

2. 如果e及f是一个环的同势元素，并且$ef = fe$，证明：ef及$e + f - ef$是同势元素。求证：属于带恒等元素的任一个环的心的同势元素关于合成$e \cup f = e + f - ef$，$e \cap f = ef$成一个布尔代数。

证：$(ef)^2=(ef)(ef)=e(fe)f=e(ef)f=e^2f^2=ef$

$(e+f-ef)^2=(e+f-ef)(e+f-ef)=e^2+fe-$
$efe+ef+f^2-ef^2-e^2f-fef+e^2f^2$
$=e+fe-e^2f+ef+f-ef-ef-ef^2+ef$
$=e+fe-ef+ef+f-ef-ef-ef+ef$
$=e+f-ef$

∴ef及$e+f-ef$是同势元素

若e,f均属于环的中心c，则ef，$e+f-ef\in c$

又因环中任意元x，$(ef)x=e(fx)=e(xf)=(ex)f$
$=(xe)f=x(ef)$

$(e+f-ef)x=ex+fx-(ef)x=xe+xf-x(ef)$
$=x(e+f-ef)$

设环中属于中心的同势元素全体记为B，则$\cup$，$\cap$在B里是封闭的，且

(i) $e\cap f=f\cap e$，$e\cup f=f\cup e$

(ii) $(e\cup f)\cup c=(e+f-ef)+c-ec-fc+efc$
$=e+(f+c-fc)-ef-ec+efc=e\cup(f\cup c)$

$(e\cap f)\cap c=(ef)c=e(fc)=e\cap(f\cap c)$

(iii) $e\cup e=e+e-e^2=e+e-e=e$
$e\cap e=e^2=e$

(iv) $(e\cup f)\cap e=e$，$(e\cap f)\cup e=e$

∵$(e\cup f)\cap e=(e+f-ef)e=e^2+fe-efe=e+fe-$
$e^2f=e+fe-ef$

同理$(e\cap f)\cup e=ef+e-(ef)e=ef+e-e^2f$
$=ef+e-ef=e$

0，1即为B的零元素和全元素。因为对B中任一元e，

$e \cap 0 = e \cdot 0 = 0 \quad \therefore e \geqslant 0$

$1 \cup e = 1 + e - e = 1 \quad \therefore 1 \geqslant e$

分配律亦成立

$\because (e \cup f) \cap g = (e + f - ef)g = eg + fg - efg$

$= eg + fg - egfg = (e \cap g) \cup (f \cap g)$

最后B是有余的

$\because e' = 1 - e$满足$e' \cap e = (1 - e)e = e - e = 0$

$e' \cup e = 1 - e + e - (1 - e)e$

$1 - e + e = 1$

故B是一个布尔代数。

3.如果对于任一环存在一个素数 p，使环里每个 a 适合 $pa = 0$ 及$a^p = a$，求证：这个环是交换环。

证：为了论证简明起见，仅就 $p = 5$ 的情形加以证明，至于一般的素数p，证明方法完全一样。

设a,b为环中任意元，于是

$$(a+b)^5 = a^5 + A_1 + A_2 + A_3 + A_4 + b^5$$

其中：$A_1 = a^4b + a^3ba + a^2ba^2 + aba^3 + ba^4$

其余A_i（$i = 2, 3, 4$）是指乘积中所有这种项的和，它的每项中b出现i次，a出现（$5 - i$）次。即A_2，A_3都包含10项，A_4有5项。由 $(a+b)^5 = a+b$，$a^5 = a$，$b^5 = b$，得

$$A_1 + A_2 + A_3 + A_4 = 0$$

上式对任意的a与b都成立，因而分别用2b，3b，4b替代b后仍然成立。而在A_i中用jb替代b后的结果是 j^iA_i。于是得出下列方程组：

$$A_1 + A_2 + A_3 + A_4 = 0$$

$$2A_1 + 2^2A_2 + 2^3A_3 + 2^4A_4 = 0$$

$$3A_1+3^2A_2+3^3A_3+3^4A_4=0$$
$$4A_1+4^2A_2+4^3A_3+4^4A_4=0$$

这方程组的系数行列式为

$$m=\begin{vmatrix}1 & 1 & 1 & 1\\ 2 & 2^2 & 2^3 & 2^4\\ 3 & 3^2 & 3^3 & 3^4\\ 4 & 4^2 & 4^3 & 4^4\end{vmatrix}$$

分别依序用这行列式中第一列元素的代数余子式乘方程组的第一、二、三、四方程后再相加起来，就得 $mA_1=0$

由于m是范德蒙行列式。$m=4!(4-3)^2(4-2)(3-2)$，它是每项都小于5的正整数的乘积，而5是素数，所以m与5互质，于是存在有整数r,s，使 $5r+ms=1$，因环的特征＝5，故有

$$A_1=(5r+ms)A_1=5rA_1+s(mA_1)=0$$

通过直接计算可得 $aA_1-A_1a=ab-ba$

由 $A_1=0$，得 $ab-ba=0$，即 $ab=ba$

［Ｇｅｎｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝抽象代数学题解
作者＝厦门大学数学系几何代数教研室代数组编
页数＝２０１
ＳＳ号＝１１１７９６１２
出版日期＝

目录